Report on selected solutions of law, business and technologies preventing crimes

11

11

11

11 11

n n

REPORT ON SELECTED SOLUTIONS OF LAW, BUSINESS AND TECHNOLOGIES PREVENTING CRIMES





Projekt *Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości,* współfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



REPORT ON SELECTED SOLUTIONS OF LAW, BUSINESS AND TECHNOLOGIES PREVENTING CRIMES

WARSZAWA 2018

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI

EDITORS PROF. RADOSŁAW KOSZEWSKI, Executive Education Center PROF. ANNA ZALCEWICZ, Warsaw University of Technology

AUTHORS

PROF. MIREIA LAS HERAS, IESE Business School PROF. RADOSŁAW KOSZEWSKI, Warsaw University of Technology, Executive Education Center PROF. TOMMASO RAMUS, Universidade Catolica Lisabon PROF. ANTONINO VACCARO, IESE Business School PROF. ANNA ZALCEWICZ, Warsaw University of Technology DR GABRIELA CIOCARLIE, Stanford Research Institute (SRI International) DR SILVIA KING, MBA I2O DR JEFF KLABEN, Stanford Research Institute (SRI International) DR ULF LINDQVIST, Stanford Research Institute (SRI International) DR LUCIEN RANDAZZESE, Stanford Research Institute (SRI International) DR ROLAND STEPHEN, Stanford Research Institute (SRI International) YAN BAI, IESE Business School DAVID BALENSON, Stanford Research Institute (SRI International) FRANCESCA CAPO, LUISS Guido Carli, Libera Università Internazionale degli Studi Social ERISIELDA DANAJ, IESE Business School BARTOSZ JANASZEK, Warsaw University of Technology MARCIN KIELISZCZYK, Warsaw University of Technology GEMMA RIERA, IESE Business School JÚLIA SIERRA, IESE Business School PIETRO VERSARI, Universidade Catolica Lisabon MARTA JANKOWSKA, Executive Education Center

REVIEWERS

PROF. DR HAB. BOHDAN JELIŃSKI, University of Gdańsk PŁK DR HAB. TOMASZ KOŚMIDER, Assoc. Prof., War Studies University in Warsaw DR HAB. KRYSTYNA NIZIOŁ, Assoc. Prof., University of Szczecin

TYPESETTING, LAYOUT: Hubert Sander

COVER DESIGN: Bogusław Słomka

ISBN 978-83-907141-7-2 © Institute of Justice Publishing House, Warsaw 2018

INSTITUTE OF JUSTICE PUBLISHING HOUSE

Krakowskie Przedmieście 25 Street, 00-071 Warsaw phone: 22 826 03 63, e-mail: iws@iws.org.pl, www.iws.org.pl

PRINTING HOUSE: Drukarnia "Elpil", ul. Artyleryjska 11, 08-110 Siedlce

TABLE OF CONTENTS

ABSTRACT	7
INTRODUCTION	9
FINANCIAL MARKET	11
Defense against Fraudulent Activities Directed at Various Institutions of the Financial Industry	11
Cybersecurity	27
Types of Cyberattacks	29
Examples of Incidents of Sector-Specific Cyberattacks and Fraud in the Banking Sectors	30
INSURANCE MARKET	35
Fraud and Cybersecurity in the Insurance Industry	35
Combating Insurance Fraud	37
Overview of Cybersecurity in the Insurance Industry	38
The Role of Technology in Fighting Fraud and Cyberattacks	41
The Role of Systemic Ecosystem Models in Fighting Fraud and Cyberattacks	43
IT Solutions for Insurance Market	48
ENERGY MARKET	57
Examples of Incidents of Sector-Specific Cyberattacks and Fraud in the Energy Sector	57
Industrial Control Systems	58
IT Solutions for Energy Market	64

MANAGING PEOPLE	69
Compliance	69
Utilization of New Technologies	92
Conclusions	97
TECHNOLOGY FOR ENTERPRISE SECURITY AND CRIME PREVENTION	99
Introduction	99
Conceptual Background	100
APPENDICES	165
BIBLIOGRAPHY	233
LIST OF FIGURES AND TABLES	239
LIST OF APPENDICES	241

ABSTRACT

This report constitutes an overview of crime-related issues present in the financial, insurance and energy sectors, and in the field of human resources management. It focuses on identifying factors linked to such changes as technological development, innovations, and influence of the operating environment which facilitate criminal behavior, and describes the latest processes, products and services implemented abroad that may contribute to reducing the probability of such crimes getting committed. The authors of the report – experts in various fields – present user recommendations and describe expected benefits and possible threats related to the use of the products and services identified in the report. One of the most important conclusions which can be drawn from the conducted research is the fact that technological development and social changes (such as society's growing sensitivity to displays of discrimination, as well as identification and criminalization of various forms of workplace harassment) have resulted in an increase in the number of reported legal violations.

The report describes various forms of "attacks" that have been or may be carried out in the financial, insurance and energy sectors, as well as different types of frauds typical for these industries (e.g. credit frauds, unsubstantiated insurance claims, etc.). Its further sections contain information on various safeguards which can be employed against such illegal activities. Significantly, the detection, prevention and defense- oriented solutions for financial and energy institutions presented in the report include not only such well-known options as user authorization and virus protection software, but also cutting-edge methods based on detection of potentially fraudulent transactions by means of behavioral analysis, big data analysis and artificial intelligence or other machine learning methods.

When it comes to people management issues, the report focused on problems related to workplace harassment and violent behavior at work. They were analyzed and divided into three categories: physical violence, psychological violence, including sexual harassment, intimidation and mobbing, and discrimination. The research has led to the following significant conclusion – on the one hand, there is a clear increase in the number of violations of employee rights, and, on the other hand, inappropriate behavior is more likely to occur in places where there is no dialogue between the management and employees, no compromise at the managerial level, and no appropriate people management policy, which creates suitable conditions for discriminatory behavior and violence to occur. The subsequent section of the report provides an overview of people management solutions based on such methods as behavioral analysis, pattern detection, as well as voice and visual analysis, which provide help during the recruitment process by identifying people's emotional states (moods) and detecting fraudulent intentions or abnormal behaviors.

INTRODUCTION

The issue of crime and relevant actions which the state can undertake to prevent and detect it, and to investigate and punish its perpetrators, remains unchangingly relevant. This constant relevance is caused by two factors. First of all, crime rates in all countries remain stable, which forces the authorities to conduct on-going investigations into the underlying causes behind this phenomena and employ broadly-understood preventive measures. Secondly, its relevance results from the fact that criminals have changed their behaviour and adapted to external circumstances (technological development, changes in social habits, development of new services, etc.). For example, research indicates that economic crime - such as credit frauds, insurance frauds and crimes related to, among others, breach of trust – is on the rise, and that the amount of cybercrime also continues to grow, including crimes consisting in illegal acquisition of legally protected data and financial fraud. The profile of the perpetrator is changing as well. Nowadays, crimes are committed by people with relevant professional background who are often employees of the affected institutions. They have high social status and specialist education ("white collar crime"). These factors combined with the high cost of crime consisting not only of the costs associated with victimization, judicial system or prevention, but also the costs arising from e.g. people losing their trust in institutions which perform significant economic functions, force the state authorities to undertake relevant actions in order to identify new methods of operation employed by criminals and adjust the prosecution methods accordingly, which means that all the people involved in detection of crimes, as well as prosecution and punishment of their perpetrators, must have appropriate knowledge and training.

The aim of this report is to present current problems related to ensuring an adequate level of security in the financial, insurance and energy sectors, and the field of human resources management. What is more, the report describes crime prevention technologies, including IT solutions, and analyses the role of compliance as a tool for managing people in organizations. Particular attention is paid to presentation of holistic solutions for identifying potential threats concerning criminal offences and preventing criminal activities.

An international team of authors – experienced experts in their respective fields, representing renowned institutions –has prepared a systematic and comprehensive overview of the indicated problems. Their involvement resulted not only in adoption of an interdisciplinary approach to the issue, but also in presentation of solutions existing in various countries. This report should be treated as an "opening report" meant to be the basis for conducting further research that would be much more focused on crime in Poland, would include more opinions of Polish experts and propose solutions that would be effective in Polish conditions.

FINANCIAL MARKET

DEFENSE AGAINST FRAUDULENT ACTIVITIES DIRECTED AT VARIOUS INSTITUTIONS OF THE FINANCIAL INDUSTRY

The presented solutions are aimed at detection, prevention, and defense against fraudulent activities directed at various institutions of the financial industry providing online services, or access to their services on the internet; these include assistance in user authorization using multichannel activity monitoring, detection of potentially fraudulent transactions by means of behavioral analysis, or analysis of large datasets by means of artificial intelligence or other machine learning methods. Presented solutions can be also used to cover a broader scope of possible forms of attacks on the integrity and compliance of financial institutions, such as money laundering activities, terrorism financing, or dishonest borrowers.

ARIC PLATFORM

Description

The proposed software platform is a process innovation for detecting crimes in financial institutions. It allows to reduce manual intervention in crime detection. It offers real-time monitoring and analysis of customer data to detect and prevent fraud by detecting behavioural anomalies. The embedded adaptive behavioural analytics module is based on machine learning and statistical modelling, which introduce a self-learning mechanism and allow to reduce manual intervention. The software builds a behavioural profile for each individual user based on the data acquired by Javascript and Mobile SDK collectors. The manufacturer offers PCI-DSS certified environment for securing customer data. The data interface is provided by means of a dedicated RESTful API available through http and https protocols. The applications of the software in question encompass identification of account takeover, prevention of social engineering attacks, such as phishing and vishing, blocking fraudulent transactions or detection of insurance application fraud.

Manufacturer's description

Name: FeatureSpace

Description: FeatureSpace Limited was founded in 2005 by David Excell, currently Chief Technology Officer and Director, and his PhD supervisor, Bill Fitzgerald, a Cambridge University Professor. The main product of the manufacturer is a software platform dedicated to fraud prevention based on behavioural analytics. The company's headquarters are located in Cambridge, UK, and Atlanta, GA, U.S. In 2018, the company was awarded for its Anti-fraud Solution of the Year at FStech Awards.

Available product options

- Software installation on customer's IT infrastructure
- Access to software via a secure web connection

Expected benefits

- Detecting and preventing account takeover and transactional frauds
- Real-time identification and blocking of phishing and vishing scams, malware attack, social engineering
- Reducing the number of manual interventions resulting in improving operational efficiency up to 50%
- Reducing the number of false positive alerts by up to 70%
- Improving customer experience by reducing unnecessary interruptions

Recommendations / users' opinions

User description: TSYS (Total System Services Inc.) is a global provider of payment services and solutions for financial and nonfinancial institutions.

Benefits/opinion: TSYS' collaboration with Featurespace aligns with our overall integration strategy.

User description: A global credit card issuer with over 1 million customers in the UK.

Benefits/opinion: "Featurespace took the time to understand what we were trying to achieve, learn about our business and come up with a solution that is going to make a real difference to our business" [3] – Global Credit Card Issuer.

User description: A leading credit reference agency in the UK.

Benefits/opinion: "The ARIC engine spots fraud better and faster. This system is clever enough to learn the behaviour of individuals and compare it with similar data, which results in far fewer false positives from abnormal behaviour and fraud activity. It makes us much more effective in what we do" [4] – Credit Reference Agency.

Sources

- www.featurespace.com/products/
- www.featurespace.com/clients/tsys/
- www.featurespace.com/clients/global-credit-card-issuer/
- www.featurespace.com/clients/credit-reference-agency/

- www.bloomberg.com
- www.crunchbase.com

BEATING eBANKING FRAUD

Description

Beating eBanking Fraud is an innovative product for theft detection in the financial field. The offered solution comprises risk-management platform for detecting and preventing transactional frauds. The working principle of the software is based on analysis of complex client profiles built with the help of behavioural analytics and machine learning. In particular, the software provides real-time monitoring of every e-banking transaction. It is especially suitable for detection of ID theft, social engineering and account takeover via malware.

Manufacturer's description

Name: Netguardians

Description: Netguardians is a Swiss company founded in 2007 and offering innovative solutions for fraud prevention and risk assessment. The company was created with the help of Swiss innovation incubator Y-Parc, in Yverdon-les-Bains, and industry investors, including Swisscom, a leading telecommunications provider in Switzerland. Currently, the head-quarters are still located in Switzerland, however the company also has branches in Nairobi, Warsaw and Singapore.

Expected benefits

- Internal fraud prevention and detection in real time
- 80% reduction in the number of false positive alerts
- Improving operational efficiency by 93%, reduction of the time needed for manual decision
- Fraud losses reduction amounting to 60%
- Rapid implementation

Sources

- www.netguardians.ch/beating-ebanking-fraud/
- www.netguardians.ch/about#the-company
- Netguardians, Beating eBanking Fraud solution brief

CR7

Description

The offered platform is a process innovation for qualifying clients as reliable in a financial institution. It is based on Nemesysco's Layered Voice Analysis (LVATM), a technology dedicated to identification of deceptive intentions by extraction of certain vocal parameters correlated with key human emotions. This solution provides real-time insight in subject's mental state and, using signal processing algorithms, enables to detect anomalies and classify them according to a certain emotional state, such as stress, excitement or confusion. It is worth noting, that the LVA is a proprietary technology of Nemesysco and can be applied over telephone lines and standard microphones. Moreover, the core technology can be adapted to various applications, including credit risk assessment and identification of potential fraudulent behaviour.

Manufacturer's description

Name: Nemesysco Ltd

Description: Nemesysco, founded in 2000, is a provider of solutions based on voice analysis technology "Layered Voice Analysis", patented by Amir Liberman, the company's CEO, which allowspersonality and risk assessment. The headquarters are located in Israel, while the offered services are globally distributed by a network of partners in over 50 business locations.

Available product options

Product is available as software for analyst's computer workstation using Voice over IP interface or connected to phone via a special connector provided by Nemesysco.

Expected benefits

- Preventing unpaid loans by identification of extra risk or potential fraudulent cases
- Increasing collectible loans by detecting positive intentions and truthfulness in cases that would be normally disqualified due to medium risk

Recommendations / users' opinions

User description: Duke University is a private institution with long academic tradition, founded in 1838. The main campus is located in Durham, North Carolina, U.S. Duke university offers a variety of highly ranked graduate programs, including Fuqua School of Business, School of Medicine and Pratt School of Engineering.

Benefits/opinion: "We find that higher levels of positive (negative) affect, as operationalized via higher levels of excitement (cognitive dissonance) determined by proprietary LVA software, convey good (bad) news about future firm performance..." [5] – William J. Mayew, Mohan Venkatachalam.

User description: University of Tsukuba is a Japanese public academic institution. The university was established in October 1973, as a result of relocation and transformation of the

Tokyo University of Education. Currently, University of Tsukuba is placed on the 250th position in QS World University Ranking.

Benefits/opinion: "Psycholosoft, a research group affiliated with the Department of Psychology at Japan's Tsukuba University, determined that Nemesysco's Layered Voice Analysis (LVA) technology is a reliable and valid tool for detecting mental stress through speech" [5] – Seishin Igaku.

User description: Mamata medical college is a private medical college, founded in 1998. The main building and teaching hospital are located in the city of Khammam, Telegana, India.

Benefits/opinion: "A significant correlation was seen between the emotional factors and certain personality traits... Thus the emotions displayed through voice can be used as a tool to determine personality" [5] – Brinda Manchireddi, Josef Kamalesh, Sumaiyah Sadaf, P. Aravind Reddy.

Sources

- · www.nemesysco.com/speech-analysis-technology
- www.emesysco.com/credit-risk-cr7
- www.nemesysco.com/about-us
- www.crunchbase.com/organization/nemesysco
- Brochures disclosed by Nemesysco staff
- · library.duke.edu/rubenstein/uarchives/history/articles/narrative-history
- www.usnews.com/best-colleges/duke-university-2920#close-modal
- · www.topuniversities.com/universities/university-tsukuba
- www.mamatamedicalcollege.com
- www.targetadmission.com/colleges/12591-mamata-medical-college-khammam

ZENSED

Description

It's an innovative real-time fraud detection platform that secures online merchant account transactions. It uses proprietary modelling software based on artificial intelligence techniques to detect potentially fraudulent transactions before they actually occur. Offered as a web-based service, it accepts information on a pending transaction from the client's payment gateway via a RESTful API, then cross-references these data with known patterns and trends, and finally returns the assessment of the transaction in terms of risk percentage of how likely it is that the transaction will have to be refunded or will cause a chargeback. Based on this information, which is accessible via an access portal to the Zensed back office, clients are able to decide whether to allow, block, or apply extra validation to the transactions marked by the model as potentially fraudulent (the information is supplied along with the basis on which the assessment was made). The AI model, which is the cornerstone of the system, automatically improves its performance over time as more transactions-

Manufacturer's description

Name: Zensed

Description: A Sweden-based start-up founded in 2015, based on the knowledge and experience of fintech professionals with strong background in the development of fraud prevention solutions. The company provides services to small clients (online merchants processing around few hundred transactions per day), as well as large ones (payment service providers, 10k to 50k transactions per day).

Available product options

Online service via RESTful API

Expected benefits

- Reduced fraud ratio at a minimized false positive rate
- Typical immediate reduction of fraudulent transaction count of more than 60%, achieving more than 80%, given that enough data is fed into the system by the client
- Operational costs reduction (with respect to services related to handling refunds and chargebacks)

Recommendations / users' opinions

- Idioscloud (an online VPN service provider)
- Mr. Jonas Hansen with GWS24
- Ms. Sara Catanzano with Borat Media, LLC (US based driver's license online renewal service)

Estimated implementation costs

- Low implementation cost (API integration with client's transaction gateway)
- Pay-per-use model: no more than 0.1 USD per analysed transaction

Sources

- www.zensed.com
- Direct electronic correspondence with Chief Executive Officer / Co-Founder Mr. Victor Fredung

FEEDZAI FOR BANKS

Description

The offered software is a real-time machine learning hybrid platform combined with a rule-based system, designed to detect anomalies on big data scale and minimize risk exposure, which is an innovative solution for financial institutions. The proposed implementation provides continuous learning mechanism for evolving customer behaviour and fraud patterns along with full risk transparency. This solution can be applied as a decision-making engine for account opening and payment authorization, which accelerates verification process with less friction and reduction of false declines.

Manufacturer's description

Name: Feedzai

Description: Feedzai was founded in 2009 by Nuno Sebastião (currently CEO), Paulo Marques (currently CTO) and Pedro Bizarro (currently CSO). According to crunchbase.com, Feedzai provides the most advanced risk management artificial-intelligence platform for ensuring banking and commerce safety. The main business offices are located in Silicon Valley, New York City, London and Lisbon.

Expected benefits

- Increased number of application approvals without an increase in fraud loss
- Reduced manual overhead, due to smaller number of false positive alerts
- · Improvement of customer service by question valuation process

Recommendations / users' opinions

User description: A Top 10 US Retail Bank

Benefits/opinion: The benefits of deployment encompass:

- A 70% increase in application approvals with zero increase in fraud loss
- 10 times fewer positive false alerts
- Acceleration of data integration from different branches

Sources

- · www.feedzai.com/solutions/retail-banks/
- www.feedzai.com/resources/case-studies/supercharging-online-account-opening-fora-top-10-us-bank/
- www.crunchbase.com

FRAUDNET

Description

A real-time online fraud management solution. Intended for digital businesses / online merchants, its goal is to increase security of processing online applications and servicing transactions by detecting fraudulent operations, including fake accounts, account takeover, or fraudulent online transactions, while keeping the trusted customers' service quality unaffected (keep customers on a "fast track"), which is a process innovation in detecting fraudulent operations. It is based on the concept of distinguishing fraudsters from legitimate consumers through multichannel analysis of the activities performed by devices used to access the monitored online services. It recognizes what device was used for accessing a service, and matches it against the black list of electronic devices. It then assesses to what extent this device corresponds with the profile of the potential, not fraudulent, customer. It is a covert, frictionless solution (i.e., transparent, requiring no additional interaction). As of 2016, the service is used by eight leading global banks and over 120 international companies across five continents.

Manufacturer's description

Name: Experian Informations Solutions, Inc.

Description: Information services company, based in Costa Mesa, California, founded in 1992 (formerly known as Information Systems and Services, Inc., changed its name in 1996), a subsidiary of Experian plc. It provides information as well as analytical and marketing services to organizations and consumers to manage the risk of commercial and financial decisions. It offers data and analytical tools that assist businesses to manage credit risk, prevent fraud, target marketing offers, and automate decision making. The company employs 17,000 people around the world.

Available product options

• Tailored on per-customer basis

Expected benefits

- Lower fraud losses
- Minimized need for manual interventions, leading to operational costs reduction
- Fraud detection rate, which is above the industry's average, discourages potential assailants/fraudsters, as proven by long-term attack rates [claim made by the company]

Recommendations / users' opinions

User description: Konstantin Guseev, Risk Director at Touch Bank in Moscow

Benefits/opinion: "We opted for Experian because FraudNet offers a sufficiently high level of customization and individual settings, ensuring high accuracy at matching suspicious devices against black lists. It is also crucial for us that the speed of assessing each device is just a few seconds. This is particularly relevant for us, since customer expectations with regard to online services are getting higher and higher every day".

User description: Anonymous Head of Fraud Technology in the Finance Industry *Benefits/opinion:* "Technically excellent but deployment must be done in the correct manner". *User description:* Anonymous Senior Product Manager in Payments & Fraud Industry *Benefits/opinion:* "Used to be a strong product but it's no longer up to ours' or the market needs".

Sources

- www.bloomberg.com/research/stocks
- https://www.experian.com/assets/decision-analytics/brochures/fraudnet-overview.pdf

- https://www.experianplc.com/media/news/2016/touch-bank-and-experian-announcea-successful-launch-of-fraudnet-to-protect-online-customers-from-fraud/
- https://www.gartner.com/reviews/market/online-fraud-detection-systems/vendor/experian-41st-parameter/product/fraudnet

SAS® FRAUD MANAGEMENT

Description

This detection solution is designed for monitoring multiple channels of data on a single platform, including payments, as well as nonmonetary events. This, together with the combination of great efficiency and real-time responsiveness, is the reason why the product is an innovation for the financial institutions. Applicability of this platform embraces handling transactions burdened with potential fraudulent behaviour. Due to deployment of machine learning mechanism along with data analytics, this solution offers real-time responsiveness in the range of milliseconds.

Manufacturer's description

Name: SAS Institute, Inc.

Description: SAS Institute is an IT company, founded in 1976, offering an advanced analytics solution for risk management, fraud prevention, customer intelligence, business analytics and data management. The headquarters are located in Cary, North Carolina, U.S., however the representative branches are dispersed all over the world, including Warsaw. The company has academic background because its foundation is a result of a project on statistical analysis led by James Goodnight, current CEO.

Expected benefits

- Increasing operational efficiency
- Improving customer experience by reducing the number of falsely declined transactions
- Reducing revenue loss

Recommendations / users' opinions

User description: HSBC is one of the largest financial institution in the world. Currently, this company provides services to over 38 million customers in 67 countries.

Benefits/opinion: "SAS is committed to ensuring that we continue to have a leading-edge anti-fraud solution. We are very pleased with the results" [2] – Derek Wylde, Head of Group Fraud Risk.

User description: Nets S/A is a European provider of digital payments and related-services, currently, having more than 300,000 partners, mainly across the Nordic and Baltic regions.

Benefits/opinion: "We've increased our fraud detection rate by 50 percent and reduced card fraud by 50 to 70 percent for cards under the optional prevention program – all while cutting false positives in half" [4] – Kaspar Kock Kristensen, Senior Vice President of Fraud and Dispute Services, Nets.

User description: Landsbankinn is Icelandic market leader in the financial services sector.

Benefits/opinion: "SAS' slogan, 'The Power to Know,' is absolutely correct. It has been a vehicle for people who don't understand the intricacies of data to begin to use it more effectively" [6] – Skuli Jensson, Head of Risk Solutions, Landsbankinn.

Sources

- www.sas.com/en_us/software/fraud-management.html
- www.sas.com/en_us/customers/hsbc.html
- www.about.hsbc.pl/pl-pl
- www.sas.com/en_us/customers/nets.html
- www.nets.eu/who-we-are
- www.sas.com/en_us/customers/landsbankinn.html
- www.corporate.landsbankinn.com/
- www.crunchbase.com

LYNX

Description

A real-time fraud detection solution for risk assessment of any monetary and non-monetary transactions. The analysis performed by the product focuses on statistical analysis of behavioural data supported by parametric analysis based on a rule-system. On the basis of data through authorization systems, Lynx evaluates the fraud risk level and generates a recommendation, which allows to reduce the client losses by providing assistance in authorization of transactions. Access to the solution is provided by intuitive and user-friendly web interface enabling fraud analysts to create fraud rules and study the risk alerts. It is worth noting that this product has been on the market for over 15 years and, according to the information provided by its manufacturer, nowadays it monitors over 25 billion operations per year.

Manufacturer's description

Name: IIC (instituto de ingenieria del conocimiento)

Description: IIC is a private institution founded in 1989 by the Asociación para el Desarrollo de la Ingeniería del Conocimiento (ADIC), an association of academic and business partners, including Banco Español de Crédito, Banco Hispano Americano, Iberia, El Corte Inglés IT, INH-Repsol, IBM, RENFE, Tabacalera, Unión Eléctrica Fenosa and Universidad Autónoma de Madrid. Currently, Instituto de ingenieria del conocimiento focuses on providing solutions for extraction of useful data based on voluminous collection (big-data) in various areas, including banking, healthcare, social media, energy and human resources.

Available product options

- Lynx program for real-time prevention and analysis
- Lynx Simulator solution for offline benchmarking risk and refusal policies before actual implementation

Expected benefits

- Achieving a high fraud detection rate
- Improving customer experience by reducing the number of legitimate transactions falsely recognized as fraudulent

Sources

- www.iic.uam.es/en/big-data-services/banking-environment/lynx/
- www.iic.uam.es/en/iic-about/who-are-we/

SAS® ANTI-MONEY LAUNDERING

Description

SAS® Anti-Money Laundering is an innovative decision-assisting tool for anti-money laundering and counter terrorism compliance departments of financial institutions. This solution employs risk-based approach, involving behavioural and peer-based analytics techniques for flow of fund monitoring, to improve accuracy and accelerate detection process.

Manufacturer's description

Name: SAS Institute, Inc.

Description: SAS Institute is an IT company, founded in 1976, offering an advanced analytics solution for risk management, fraud prevention, customer intelligence, business analytics and data management. The headquarters are located in Cary, North Carolina, U.S., however the representative branches are dispersed all over the world, including Warsaw. The company has academic background because its foundation is a result of a project on statistical analysis led by James Goodnight, current CEO.

Available product options

- SAS® Anti-Money Laundering [details pending]
- SAS® High-Performance Anti-Money Laundering (Distributed LASR) [details pending]
- SAS® High-Performance Anti-Money Laundering (Non-distributed LASR) [details pending]

Expected benefits

- Accelerating strategy validation by means of transparent visualization flow of funds and alert origin
- Increasing detection efficiency by higher alert quality and accuracy (improving SAR conversion up to 4 times in midsize institutions)

Recommendations / users' opinions

User description: Landsbankinn is Icelandic market leader in the financial services sector.

Benefits/opinion: "SAS' slogan, 'The Power to Know,' is absolutely correct. It has been a vehicle for people who don't understand the intricacies of data to begin to use it more effectively" – Skuli Jensson, Head of Risk Solutions, Landsbankinn.

User description: Laurentian Bank of Canada is a leader in providing banking products and services in the Canadian market.

Benefits/opinion: "Cross-referencing across several cases and identities tells you you're dealing with a criminal network" – Robert Quevillon, Assistant Vice President of Corporate Security, Laurentian Bank.

Sources

- www.sas.com/en_us/software/anti-money-laundering.html
- www.sas.com/en_us/customers/landsbankinn.html
- www.corporate.landsbankinn.com/
- www.sas.com/en_us/customers/laurentian.html
- www.laurentianbank.ca/en/about_lbc/my_bank/our_image.html

RIALTO

Description

Exeura provides a solution based on their analytical platform Rialto. By means of machine learning techniques as well as descriptive and predictive analysis, Rialto software provides assistance for analysts in all phases of decision-making process, which is a process innovation. The offered solution can be integrated in the third-party applications operating on data of various types and formats. Applicability of this platform covers detection of anomalies and suspicious behaviour, which is suitable for risk assessment for the purpose of detecting money laundering and terrorism financing.

Manufacturer's description

Name: Exeura

Description: Exeura s.r.l. was founded in 2000 as a research spin-off from the University of Calabria, Italy. The company still maintains connections with academics, as the president of Exeura, Pasquale Rullo, is a professor at University of Calabria. Exeura provides business analytics solutions based on exploring and processing voluminous sets of data.

Expected benefits

- · Monitoring and building models of typical customer purchasing behaviour
- Management of customer profiles concerning prepaid cards usage
- · Assessment of risk indicators for each customer

Recommendations / users' opinions

User description: Business activity of CartaLis is focused on providing prepaid cards and related services. Currently, CartaLis is a part of IGT PLC group, a leader in the Italian regulated gaming market.

Benefits/opinion:

- 70% time reduction in suspicious-behaviour alert generation
- Increased productivity of analysts: from 2.7 hour per report to 1.8 second per report
- Errors in data transcription reduced to zero
- · Ability to monitor the entire customer database

Sources

- http://www.exeura.eu/en/solution/risk-analysis/
- http://www.exeura.eu/en/exeura/about-us/
- · https://www.lottomaticaitalia.it/en/about-us/media/company-profile
- · https://www.lottomaticaitalia.it/en/about-us/company/company-structure

SEON FRAUD API

Description

SEON is a fraud detection solution dedicated to online merchants, made of 4 highly independent functional innovative units delivered in the form of APIs: (1) Label API, which collects post-back data from client's payment gateway which, together with other metrics associated with the transaction, are used to train the decision-making engine, (2) Proxy API, providing assessment of risk associated with an IP address (here: a unique address unequivocally identifying a user or a group of users) used to access the service, (3) Email API, used for e-mail address investigation by means of social media profiling and analysis of data aggregated from various open sources, and (4) Device Fingerprinting, which collects data related to devices associated with a particular user. The company's flagship product, Fraud API, integrates all the aforementioned solutions into a single API. The relevant data is delivered to the user through web application (Admin Panel), allowing for manual transaction review. As an option, clients can choose to anonymously share fraud patterns and analysis reports with other clients to improve the effectiveness of the solution. The company does not provide chargeback guarantee.

Manufacturer's description

Name: SEON Technologies Ltd.

Description: SEON is a Hungarian technological start-up founded in 2015. It is based on its founders' experience (Tamas Kadar and Bence Jendruszak) in working at a bitcoin exchange, where they made observations of fraudulent activity resulting in a high chargeback rate. The company's operations are focused on (but not limited to) the European market.

Available product options

A set of 4 core APIs is offered, of which any subset can be selected for integration with client's platform.

Expected benefits

- Ease of integration at various "action points" (i.e. at the signup stage, account login or data edition, etc.) [1]
- Low fee per API call (no chargeback compensation included)

Recommendations / users' opinions

User description: OTP Bank – the largest commercial bank in Hungary (with total assets of around USD 48B as at the end of Q4 2017), offering a full range of services to individual and corporate clients in Central and Eastern Europe.

User description: Gránit Bank – a Hungarian bank for individual as well as corporate clients (at end of 2017 total assets of USD 832M) [2].

User description: eShield - a U.S. based building insulation solutions provider [3].

User description: Buffered Ltd. – a global VPN service provider.

User description: Koninklijke Luchtvaart Maatschappij N.V. (aka KLM Royal Dutch Airlines) – the Netherlands flagship carrier airline, member of the SkyTeam alliance, the oldest airline in the world's history.

User description: Eurobet Italia SRL – a major operator of online bets in Italy and a part of Coral Eurobet Group [5].

Estimated implementation costs

- Low implementation cost (API integration with the client's platform)
- Payment per API request, depending on the monthly request volume (but no more than EUR 0.08 per request)

Sources

- www.seon.io/products/fraud-api/
- www.granitbank.hu/upload/hirdetmenyek/Nyilvanossagra%20hozatal_2016_web.pdf
- www.eshield.net/about-us.html
- https://www.icelondon.uk.com/exhibitor-press-releases/seon-moving-from-bitcoin--to-advanced-fraud-solution#/
- http://www.eurobet.it/guida/informazioni/chi-siamo.html

THE DEEPEYES SOLUTION

Description

The DeepEyes solution is an innovative product, artificial intelligence (AI) platform, designed to detect the emotional state of a subject through analysis of micro expressions. Real time analysis is provided by combining statistical and mathematical modelling together with machine and deep learning technologies. Relying on the data acquired by a simple HD camera, the software conduct analysis of video material and performs face recognition, as well as, emotions identification. By means of AI-assisted video processing, this solution provides biometrical identification and emotional state assessment, which is suitable for additional authorization process, access control and verification of potential borrowers' truthfulness.

Manufacturer's description

Name: DeepEyes

Description: DeepEyes is an IT solution provider for risk assessment and business analytics. The main product offered by the company is software designed to perform computer vision analysis. The company was founded in 2015 and, currently, actively operates in Germany, the Netherlands and the United Kingdom.

Available product options

Since the DeepEyes algorithm is relatively undemanding, the software can be installed on a conventional computer workstation or a mobile device equipped with an HD camera. Moreover, the software does not require an Internet connection.

Expected benefits

- · Improved customer service by means of accelerated biometric authorization process
- Improved fraud detection rate
- · Decrease of losses resulting from unsettled loans

Sources

- www.deepeyes.co/industries/
- www.deepeyes.co/industries/financial_industry/
- www.deepeyes.co/deepeyes_team/
- www.crunchbase.com/organization/deep-eyes

RISKIFIED FRAUD DETECTION SOLUTION FOR ECOMMERCE

Description

Riskified offers a chargeback protection platform dedicated to online merchants based on a self-optimizing machine learning model particularly aimed at behavioural analysis (Spektra model). The detection process also comprises proxy detection, device fingerprinting and social media analysis as supplementary countermeasures. As opposed to other anti-fraud solutions its business model concentrates on providing an insurance policy against fraudulent transactions rather that the technology used to provide it to its clients.

Its operation principle is as follows: If the transaction is misclassified by the system (i.e., a fraudulent transaction is allowed for further processing), Riskified will cover the resulting

chargeback, i.e., it offers full chargeback guarantee to the merchants on the approved transactions, which is a distinctive feature among other fraud detection/prevention solutions.

Manufacturer's description

Name: Riskified

Description: Riskified is an Israeli technological/fintech start-up, currently based in New York, USA. It was founded in 2013 by Eido Gal and Assaf Feldman. Its investors include: Pitango Growth, Capital One Growth Ventures, Qumra Capital, Genesis Partners, Groupe Arnault, C4 Ventures, The Phoenix Insurance Company, NTT DOCOMO Ventures, and Entrée Capital. The company was voted a winner of 2016 METAward Merchant Risk Council (MRC) meeting [4].

Note: Merchant Risk Council is a not-for-profit group of over 500 member organizations focused on providing services and solutions for reducing eCommerce fraud.

Available product options

- Integration of an API within the client's existing framework (sales system, transaction gateway), or
- eCommerce platforms

Expected benefits

- Predictable operational risk thanks to the chargeback guarantee
- 30% rise in sales [1]
- 66% fewer declines on valid transactions (reduced false-positive ratio)
- Frictionless review process (instant transaction review)

Recommendations / users' opinions

User description: Burberry – a British fashion house and a globally recognized luxury clothing brand [2].

User description: Macy's – an American department store chain founded in 1858, one of the largest retailers in the USA [2].

User description: lastminute.com NV (aka lastminute.com group) – online travel booking search engine, founded in 2004, currently employing 1,200 people in 12 countries and offering services in 40 countries. It provides services to around 10 million passengers yearly. Its group's revenue totalled EUR 251.3M in 2017 [3].

Estimated implementation costs

- As an API-based solution, its implementation costs are comparatively low, depending on the particular client's case
- Pricing depends on client's sales volume and the unique risk profile of the industry in which the client operates

Sources

- https://www.riskified.com/solution/
- https://www.bizjournals.com/newyork/news/2017/06/27/riskified-raises-33-millionfrom-pitango-growth.html
- http://www.lastminutegroup.com/~/media/Files/B/Bravofly-Rumbo-Group/reportsand-presentations/2018/lastminute_Annual_Report_2017.pdf
- https://www.merchantriskcouncil.org/news-and-press/press/2016/2016-metaward-winners

CYBERSECURITY

Cybersecurity is defined by The Committee on National Security Systems (CNSS) Glossary Working Group simply as "[t]he ability to protect or defend the use of cyberspace from cyberattacks"¹. This definition is also adopted by National Institute of Standards and Technology of the United States (US) Department of Commerce.² The occurrence of cyber-related attacks is escalating and is associated with increasing costs, reputational and other risks. It is also widely understood that cybersecurity incidents and a great bulk of data security breaches are becoming more striking and severe.

"As we do more and more of our business online, and as criminals realize the value of the data that organizations are protecting, we're seeing more big-name breaches, more high-profile breaches" – Mark Nunnikhoven, vice president of cloud research at the security company Trend Micro³.



Figure I.1. Cyberthreat awareness and preparedness

Source: Accenture Research

¹ https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

² https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

³ http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

Figure I.1 is based on 2015 data from an Accenture's Global Risk Management Study⁴ (Accenture Study) which shows the levels of perceptions, preparedness and awareness in understanding and addressing cyber-related threats.

An overview of types of cyberattacks and trends in data breaches is shown in Figure I.2 below, from the Identity Theft Resource Center 2017 Annual Data Breach Year-End Review. The graphic "captures seven different types of attacks: hacking (with subcategories of phishing, ransomware/malware and skimming), unauthorized access, insider theft, and data on the move, accidental exposure, employee error/negligence/improper disposal/loss, and physical theft. Hacking continues to rank highest in the type of attack, at 59.4 percent of the breaches, an increase of 3.2 percent over 2016 figures"⁵.



Figure I.2. Overview of types of cyberattacks and data breaches

Source: Cybersecurity and Fraud in the Banking and Energy Sectors, Current landscape, best practices and organizational approaches – and options for Poland, A. Vaccaro, S. King

The magnitude of the impact losses from cyberattacks are both under-reported and difficult to measure because, in addition to direct costs and financial losses, there are intangible effects such as reputational consequences for companies and institutions, and ever-evolving risk amplifications throughout important industry sectors and the overall national and global landscape.

⁴ https://www.accenture.com/_acnmedia/Accenture/next-gen/top-ten-challenges/challenge9/pdfs/Accenture-2016-Top-10-Challenges-09-Cybersecurity.pdf#zoom=50

⁵ https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

"A key finding of our 2018 report is that nearly half (46 percent) of organizations rarely make substantial changes to security strategy – even after being hit by a cyberattack. This represents a failure to learn from past incidents that puts sensitive data, infrastructure and assets at risk; a consequence that respondents recognized, with the same proportion – 46 percent – saying their organization can't always prevent attackers from breaching internal networks"⁶ – CyberArk February 28, 2018.

It is, therefore, important that companies and institutions properly address mitigating the exposure to cybersecurity threats. This, as discussed in this paper, means transcending current organizational inertia and actively seeking frameworks, technologies and programs to maintain proper controls and stewardship over organizational data and systems.

TYPES OF CYBERATTACKS

There are many different lists of types of cyberattacks. Below, we leverage the UK IT Governance organization's list and definitions⁷.

Ransomware

Ransomware is a type of malicious software that demands a ransom fee be paid after the software is installed on a computer system. This type of malware is very common.

Viruses

A virus is a piece of malicious code that is loaded onto a computer without the user's knowledge. It can replicate itself and spread to other computers by attaching itself to another computer file.

Worms

Worms are similar to viruses in that they are self-replicating, but they do not require a program to attach themselves to. They continually look for vulnerabilities and report back any weaknesses that are found to the worm author.

Spyware / adware

Spyware/adware can be installed on your computer without your knowledge when you open attachments, click links or download infected software. This malware then monitors your computer activity and collects personal information.

Trojans

A Trojan virus is a program that appears to be for a certain function, but is actually performing malicious activity when executed. Trojans are often disguised as virus removal programs.

⁶ https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018-business-view-security/

⁷ https://www.itgovernance.co.uk/blog/different-types-of-cyberattacks/

Attack vectors

Attack vectors are used to gain access to a computer or network in order to infect computers with malware or harvest stolen data. These vectors come in three main forms:

• Social engineering

Social engineering – is used to deceive and manipulate individuals in order to gain computer access. This is done by making individuals click malicious links or by physically gaining access to a computer through deception. Two examples of social engineering are:

Phishing – This is an attempt to access sensitive information such as passwords and bank information by disguising as a trusted individual. This is done via electronic communication, most commonly by email.

Pharming – This is an attack that redirects a website's traffic to a fake website, where users' information is then compromised.

• Drive-by

A drive-by cyberattack targets a user through their Internet browser, installing malware on their computer as soon as they visit an infected website. It can also happen when a user visits a legitimate website that has been compromised by hackers. They are then infected directly from that site or redirected to a malicious site.

• Man in the middle (MITM)

An MITM attack is where an attacker alters the communication between two users, impersonating them both to manipulate both victims and gain access to their data. The users are not aware that they are not talking to each other, but are actually communicating with an attacker. For the purposes of this paper, this list and brief descriptions shall serve as sufficient to help frame the discussion of best practices for mitigation.

EXAMPLES OF INCIDENTS OF SECTOR-SPECIFIC CYBERATTACKS AND FRAUD IN THE BANKING SECTORS

Recent and salient examples, to pick a few from the plethora of events, include:

- 2018: City of Atlanta: "Atlanta Paralyzed For More Than A Week By Cyber Attack"⁸. The City of Atlanta is the fulcrum of a metropolitan area of approximately 6 million people the 9th largest in the US.⁹ The economic cost of crippling the City's ability to conduct business has been enormous and the reputational implications have been grave and are yet to be fully understood.
- 2017: Equifax: "Cybercriminals penetrated Equifax..., one of the largest credit bureaus [in the US], in July and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including Social Security numbers"¹⁰.

⁸ https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-week-by-cyber-attack

⁹ http://worldpopulationreview.com/us-cities/atlanta-population/

¹⁰ http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

 2017: NotPeya: "The NotPetya ransomware targeted companies in Ukraine, attacking its government, financial and energy institutions last June. It ended up causing collateral damage to global companies with offices in Ukraine, including Maersk, FedEx and Merck. The cyberattack ended up costing Maersk up to \$300 million in lost revenue"¹¹.

Financial Sector

"For years, the financial services sector globally has been a primary target for attacks by cybercriminals largely because of the tremendous value of the information available. In fact, financial services firms are reportedly hit by cybersecurity incidents a staggering 300 times more frequently than businesses in other industries...[and] the cost to a financial institution facing a cyberattack specifically targeting their online banking services costs an average of \$1.8 million" according to reports by the Identity Theft Resource Center¹².

Fraud and types of fraud have been presented in the Fraud section above – and remain a large portion of crimes committed against banking institutions and customers. Like the Energy industry, the Banking industry is less than prepared.

"As for quantifying losses from data breaches, banks have long expressed a need for better tools in making these calculations. For all the time and resources invested in models to estimate potential losses from market and credit risks, many firms are unable to measure their exposure to data breaches"¹³ – Risk.net, 2018.



Figure I.3. Top operational risks for 2018

Source: https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

¹¹ https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

¹² https://cdn2.hubspot.net/hubfs/524149/Gated_Content/financial%20white%20paper%202017%20FINAL%20 Pages.pdf?submissionGuid=94df83ac-02df-41dc-ba2f-2e0c179ae533;http://us.generaliglobalassistance.com/ blog/white-paper-impact-cybersecurity-incidents-financial-institutions/

¹³ https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

Additionally, the Banking sector continues to recognize that cyber-threats and fraud – with all associated regulatory compliance, are top of mind perceived risks, as illustrated from Figure I.3 (also from Risk.net).

Typically, individuals target the Banking sector because... that's where the money is: "Financial institutions are prime targets for cyberattacks"¹⁴ and fraud is often the primary type of economic crime committed against financial institutions. Fraud is a significant factor in the Banking sector and, as Figure I.4¹⁵ below shows that remote banking is, by a large margin, the main culprit.

The authors recommend accountable leaders take action and proactively adopt a sound and comprehensive information assurance program (such as Community Gold Standard presented here – Appendix 1, Appendix 2, Appendix 3) and that they do so with a mindset and sensibility to owning, engaging in, and driving the ongoing global conversation stakeholders have launched.

Figure I.4. 2016 financial fraud losses by type



Source: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf

Other agents may cyberattack banks and financial institutions with the intent of obtaining valuable personal information about customers or, in more severe cases, to disrupt the functioning of financial markets. Here are a few headlines that showcase the specific and emerging exposure to cyberattacks and fraud (including physical) by the Banking sector:

• Seven UK banks targeted by co-ordinated cyberattack, Financial Times, April 25, 2018

"Seven of the UK's biggest banks including Santander, Royal Bank of Scotland and Tesco Bank were forced to reduce operations or shut down entire systems following a cyberattack"¹⁶.

¹⁴ https://www.wsj.com/articles/why-we-have-to-really-worry-about-the-banks-cybersecurity-1513652881

¹⁵ https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf

¹⁶ https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb

• The Impact Of Cyber Attacks On The Banking Industry, WallStreet.com, Jan 26, 2018

"Banking Sector Most At Risk. Of course, the banking sector is one of the industries that are most at risk, given the nature of the data that they hold. This means that banks have had to dedicate significant funds on developing their digital infrastructure to strengthen their cybersecurity"¹⁷.

• ATM Raiders Jailed In Joint Cross-Border Investigation, Europol, April 2018

"Since 2015 Germany has seen a major uptake of criminal gangs coming from the Netherlands to commit ATM attacks"¹⁸.

In this paper we aimed to provide an overview of cybersecurity and fraud challenges in the Banking sectors; deliver recommended best practices tools; and guide the reader through a journey of understanding key aspects to be considered when establishing and/or improving cyber and fraud management capabilities.

The adaptive demands of having sound information assurance practices cannot be underestimated. Companies operate with such level of expectations and scrutiny – not to mention consequences – over their data protection and usage practices that, for example,

"Facebook [had] to Reorganize After Scrutiny Over Data Privacy" just a few weeks after the recent Cambridge Analytica data scandal. While Facebook's core business may not reflect that of the Banking industry, the message is the same: A corporation and its leadership are responsible and accountable for their data set management practices like never before – and need to adapt.

The authors recommend accountable leaders take action and proactively adopt a sound and comprehensive information assurance program (such as Community Gold Standard presented here) and that they do so with a mindset and sensibility to owning, engaging in, and driving the ongoing global conversation stakeholders have launched.

¹⁷ https://wall-street.com/impact-cyberattacks-banking-industry/

¹⁸ https://www.europol.europa.eu/newsroom/news/atm-raiders-jailed-in-joint-cross-border-investigation
INSURANCE MARKET

FRAUD AND CYBERSECURITY IN THE INSURANCE INDUSTRY

Insurance fraud occurs when individuals intentionally misrepresent claims to deceive an insurance company to receive money they are not entitled to¹. "Fraud [then] is a deliberately dishonest act that causes actual or potential financial loss to any person or entity"². Fraud in the insurance industry impacts everyone – as the losses associated with fraud are reflected in higher insurance premiums.

"Insurance fraud is hardly a victimless crime. When dishonest people take money they don't deserve from insurance companies, this act results in increased policy cost for every-one".

Source: Pennsylvania Insurance Fraud Prevention Authority, 2018³

Typically, insurance fraud spans from an individual inflating claims with higher than incurred loss values or withholding information that can affect the valuation of the claim – to fraud committed through the activities of organized persons who employ material and complex methods to submit false claims. Specifically, insurance fraud can be:

- *Opportunistic* the padding and exaggeration of otherwise legitimate claims
- Premeditated arson, theft, staged incidents involving the deliberate fabrication of a claim
- *Fraudulent non-disclosure* misrepresentation of facts material to the insurance policy, such as failure to disclose a criminal conviction or giving deliberately misleading information in support of a claim"⁴.

Common examples of insurance fraud are listed below (from the US source Criminal Defense Lawyer⁵):

¹ https://www.criminaldefenselawyer.com/crime-penalties/federal/Insurance-Fraud.htm

² https://www.criminaldefenselawyer.com/crime-penalties/federal/Insurance-Fraud.htm

³ http://www.helpstopfraud.org/What-is-Insurance-Fraud/Impact#

⁴ http://understandinsurance.com.au/insurance-fraud

⁵ https://www.criminaldefenselawyer.com/crime-penalties/federal/Insurance-Fraud.htm

Healthcare

This occurs when a person or business defrauds a health insurance provider and also commonly occurs when health care providers submit claims to a health insurance provider for procedures they did not actually perform. As well as being a crime in all fifty US states, health care fraud is also illegal under federal law.

Automobile claims

This occurs when someone either exaggerates or fabricates a claim made to their automobile insurance provider. For example, a person may claim that the extent of damage that occurred in an automobile accident was greater than it actually was, in order to obtain a larger payment from the insurer.

Life

This happens when a person attempts to obtain life insurance payments by fabricating their own or another's death. For example, a person who forges a death certificate of a family member to obtain his life insurance payment.

Figure II.1. Fraudster Profile

PERSONAL

- Undergoing known financial difficulties
- Divorce or other major life changing events
- Unexpected change in behavior
- Instability in their life circumstances
- Past employment related problems
- Past legal problems
- Living beyond their means or an excessive lifestyle
- Desire for personal financial gain
- Excessive family or peer pressure for success

PROFESSIONAL

- Unusually close relationship with vendors or clients
- Serves as primary contact with law firm bank and payroll vendor
- · Often makes tasks more difficult than necessary perhaps 10 obfuscate or reduce transparency
- Overly protective about their workplace
- · Prefers lo work unsupervised, after regular work hours or frequently lakes work home
- · Complains about lack of authority or a micro-managing work environment
- Complains about inadequate pay
- Complains about excessive work pressure and stress
- Reluctance to take vacations or extended time away from the office

PERSONALITY TRAITS

- Control issues manifested in such ways as an unwillingness to share duties or asking fellow
 employees not to go through their mell or work product while they are out of the office
- Excessive secrecy or trust Issues
- · Irritability, suspiciousness or defensiveness
- Confrontational when challenged
- Tells lies even about unimportant items
- Unreliable
- Cuts corners or bends the rules
- Tends lo shift blame and offer excuses

Source: http://www.lawyersmutualnc.com/blog/profile-of-a-fraudster

Property

This is fraud concerning home, business, or other insurance policies covering real property (land or buildings) or personal property. A business owner who sets fire to his own business has committed this type of fraud. An owner of a valuable piece of jewelry may claim that the item was lost, in order to obtain a payment. Property insurance fraud may also include exaggerating the damages from a legitimate loss – for example, a person who had a pipe burst in his home might claim damages in excess of those that actually occurred.

Who commits fraud? What are the characteristics of an insurance fraudster? Figure II.1, from the US-based Lawyers Mutual⁶, which provides programs for claims prevention education, illustrates the profile of fraudsters and identifies the "red flags" that trigger fraud.

It is important to note that there are two categories which the insurance industry and enforcement agencies classify as acts of fraud: "Soft insurance fraud" and "Hard insurance fraud". Figure II.2 puts the distinction between the two types of insurance fraud into context by providing examples.

Figure II.2. Soft and Hard Insurance Fraud



Source: https://www.pinow.com/articles/1666/the-difference-between-soft-and-hard-insurance-fraud

The civil and criminal consequences of committing insurance fraud vary by type of fraud and by legal constructs across the world.

COMBATING INSURANCE FRAUD

According to Insurance Europe, which is a European insurance and reinsurance federation with 34 member bodies – the national insurance associations – that represents all types of insurance and reinsurance undertakings"⁷, the types of responses and approaches to combating fraud are different from country to country. While this source is focused on Europe, this list is applicable globally. A condensed list of the types of responses cataloged is found below. Appendix 4– Insurance Europe:

Combating Fraud, provides a full, informative extract from the report (Impact of Insurance Fraud, $2013)^8$ – with details about the list below and country-specific examples. Identified tactics to combating insurance fraud in Europe, then, include:

⁶ http://www.lawyersmutualnc.com/blog/profile-of-a-fraudster

⁷ https://www.insuranceeurope.eu/about-us

⁸ https://www.insuranceeurope.eu/sites/default/files/attachments/The%20impact%20of%20insurance%20fraud.pdf

- Insurers exchanging relevant information about fraud events
- Cross-border cooperation via formal and informal groups to investigate insurance fraud
- Setting up national bodies, like the *Agence pour la lutte contre la fraude à l'assurance*, (ALFA) in France, to investigate suspicious claims these bodies also deliver training and certification of fraud investigators and advice
- Creating corporate investigation units
- Appointing fraud representatives in insurance organizations
- Establishing bureaus to lead or co-ordinate industry response to criminal fraud networks
- Increasing co-operation with law enforcement agencies within and across countries
- Devising easy visual checks to identify possible stolen vehicles
- Reporting all identified fraud to the police
- Initiating "protocols" of cooperation with international reach
- Funding insurance fraud units at respective law enforcement agencies
- Using advanced key-readers to confirm that vehicle claims are valid
- Using social medial platforms, like Facebook, to uncover potentially fraudulent injury and other claims
- Training insurance staff, the police, other authorities and the media including recurring training of front-line claims adjusters
- Organizing and offering seminars on insurance fraud
- Implementing the use of "cheat-lines" (hotlines, typically anonymous) to report suspected or known insurance fraud
- Increasingly using technology to uncover fraud

Before addressing best practices in fighting fraud with a lens towards the role of technology and the design and implementation of sound corporate strategies, the section below, "Overview of cybersecurity in the Insurance Industry", introduces and delves into the additional risk factor, not unique to the insurance sector and increasingly occurring, which is the exposure to cyberattacks aimed at compromising the integrity of the data governed by an organization. There is an important link between exposure to fraud and cyber vulnerabilities – data management practices and governance – which is a vital component of any best practices for deference against both fraud and cyberattacks.

OVERVIEW OF CYBERSECURITY IN THE INSURANCE INDUSTRY

Like other institutions, insurers are under pressure to address issues of data breaches resulting from cyberattacks. According to a Deloitte case study⁹ "[c]yber-attacks in the insurance sector are growing exponentially as insurance companies migrate toward digital channels in an effort to create tighter customer relationships, offer new products and expand their share of customers' financial portfolios... [and] the challenges are likely to become more complex

⁹ https://www2.deloitte.com/be/en/pages/risk/articles/insurance.html#

as insurers embrace big data and advanced analytics that require collecting and handling vast amounts of consumer information." The case study article is based on a sample of three cases of cyber exposure that are frequently surfacing as issues for insurers and other financial institutions: failure to protect customer data, and improper access to credit card information and Social Security numbers.

Appendix 5 – from the Deloitte Case Study, offers a summary of the three cases explored.

Another recent study by the consulting firm Protiviti, "Cybersecurity Regulatory Issues in the Insurance Industry"¹⁰, further notes that insurers are currently subject to two specific forms of cybersecurity-related pressures: 1. Regulatory pressure and 2. Modernization, innovation and cybersecurity.

Figures II.3 and II.4 below articulate the dimensions of the "Call to Action" relating to these pressures:

Regulatory pressure

The Protiviti study is based on the US market, where insurers are regulated by the states in which they operate. While regulatory efforts differ across the globe, the regulatory initiatives listed below can indicatively be representative of efforts in other countries and cross-national agencies. Here are examples of a recently enacted regulation:

- In 2015, the National Association of Insurance Commissioners (NAIC) established
 a Roadmap for Cybersecurity Consumer Protections¹¹ which "describes the protections the NAIC believes consumers are entitled to from insurance companies,
 agents and other businesses when they collect, maintain and use [consumers] personal information, including what should happen in connection with a notice that
 personal information has been involved in a data breach." The summary document
 can be found in Appendix 6 2015 NAIC Roadmap for Cybersecurity Consumer
 Protections. Since publishing the Roadmap, NAIC launched a series of projects respectively aimed at setting guidelines to: a) articulate insurance regulators' strategy
 regarding cybersecurity¹²; b) improve data security review and analysis by financial examiners (in the context of statutory or firm established period examinations);
 c) place formal protocols to collect and analyze data on cybersecurity vulnerabilities
 in the industry; and d) devise a roadmap for industry players to protect consumers
 from cybersecurity exposure.
- It is worth noting that the regulatory landscape around data protection is shaping quickly and materially. For example, in 2017, the US National Association of Insurance Commissioner enacted The Insurance Data Security Model Law¹³ (draft found in Appendix 7), and, in May 2018, the European Union enacted the General Data Protection Regulation (GDPR), which "regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU"¹⁴.

¹⁰ https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity-regulatory-issues-in-theinsurance-industry-protiviti.pdf

¹¹ http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_ protections.pdf

¹² http://www.naic.org/documents/committees_ex_cybersecurity_tf_160524_draft_ins_data_sec_model_law.pdf

¹³ http://www.naic.org/store/free/MDL-668.pdf

¹⁴ https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulationgdpr-govern_en

This legislation presents with aggressive goals towards protecting companies and consumers from data breaches.

It is not in scope for this paper to fully address the data and privacy regulatory landscape, however, both the fact that, "[M]ayor cybersecurity breaches have become routine as organizations rely increasingly on vulnerable digital technologies and third- party providers"¹⁵, and that legislative pressure is increasing worldwide¹⁶, highlight and provide context for the content presented in sections following.

Figure II.3. Cybersecurity regulation: Call to Action

Call to Action	
This rapid development of cybersecurity "rules of the road" by America's insurance regulators requires boards of directors and senior management of insurance companies to think critically about a number of risk and compliance related issues, including:	
How will their organization's cyt	tion perform on a statutory or targeted financial exam concerning a review of er posture and data security?
If they are licensed in t cybersecurity process	रिष्फ York, how will they perform on a NYDFS review or examination of their es and protocols?
Once the NAIC model in a state's review or example.	s in place and starts to be adopted in more U.S. states, how will they perform on nination of their cybersecurity processes and protocols?
If they sell any cyber liz to insurance regulators	bility insurance products, will the information they are now required to disclose raise any questions that they will need to be prepared to answer or address?
It is far better for an insurance company to know the answer to these four questions, as well as take any necessary proactive steps, before a damaging data breach happens or before an insurance regulator commences a review and/or examination.	

Source:https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity-regulato-ry-issues-in-theinsurance-industry-protiviti.pdf

Modernization, innovation and cybersecurity

The statement below, from the Protiviti study¹⁷, well frames the nature of the challenge when addressing issues of modernization and innovation in the organizational construct of insurance companies.

"Insurers, grappling with low interest rate environment, are seeking to cut costs and drive product innovation to tap into new sources of revenue. Modernizing legacy systems enables firms to leverage new technology and improve their product offering and customer experience, but it also generates new risks and control challenges".

¹⁵ https://www.protiviti.com/US-en/insights/security-threat-report

¹⁶ https://www.bluefin.com/bluefin-news/global-cybersecurity-laws-regulation-changes-2018/

¹⁷ https://www.protiviti.com/US-en/insights/security-threat-report

The risks addressed in the statement revolve around the adoption of sophisticated cloud based data tools, which may introduce the need to have a data protection strategy that is well thought out, and which is compliant with current data security standards (such as those set out in the ISO/IEC 27001 – the best-known standard providing requirements for an information security management system¹⁸ – An overview is presented in Appendix 8) as well as the regulations mentioned above. Hence, it is important that insures pay particular attention to the design of privacy controls and to risk management practices addressing vendors and outsourcing ventures.

Figure II.4. Cybersecurity innovation: Call to Action

Call to A	ction
The rapid more pray dedicated the follow	growth of third-party providers and the increased risk they pose requires firms to adopt a gmatic approach to adequately control the risk without exhausting their limited resources I to managing third-party risk. To better manage this risk, insurance companies need to consider ring four key action points:
01	Ensure security is appropriately included in modernization plans. Make sure security representation is included in the planning and project execution phases.
02	Recognize security models will need to change with new areas such as agile and cloud adoption. Begin work early to understand and incorporate appropriate controls into the plans. Acknowledge that these are new areas which may require expertise not currently on staff. Additional training and education may be required to ensure the organization can address these new areas.
03	Consider how regulators will examine these modernized environments using the new frameworks. Begin gap assessments of the modernized environments early in the process to ensure appropriate controls, evidence and governance will support imminent examinations.
04	Begin to inventory and assess third-party providers to understand the risks they pose and develop a risk management plan.

Source: Tommaso Ramus, Fraud and Cybersecurity in the Insurance Industry, 2018

Having painted a picture of the landscape surrounding fraud and cybersecurity issues in the insurance industry, the remainder of the paper explores, in more detail, how insurers can leverage best practices in technology and organizational design strategies to mitigate and combat fraud and cyberattacks exposure.

THE ROLE OF TECHNOLOGY IN FIGHTING FRAUD AND CYBERATTACKS

As noted by The Digital Insurer publication "The insurance industry and technology are no strangers to each other. And yet the industry has not been considered a leader when it comes to the application of technology."¹⁹ Additionally, "[c]yber fraud continues to be a growing issue for insurer anti-fraud departments". For further context, Appendix 9 contains an extract

¹⁸ https://www.iso.org/isoiec-27001-information-security.html

¹⁹ https://www.the-digital-insurer.com/blog/10-insurtech-trends-insurance-2018/

from the "The State of Insurance Fraud Technology"²⁰ – A study of insurers' use of, strategies, and plans for anti-fraud technology, 2016, conducted by The Coalition Against Insurance Fraud, which presents a snapshot of the current state of fraud and technology.

A thorough scan of research on best practices, and technological innovation trends in the insurance industry surfaced a recent study by the consulting firm EY^{21} that, among the many, perhaps best serves in framing the discourse in this paper. Figure II.5 identifies five "buckets" of key insurance technology trends. Each of the five trends are summarized below and Appendix 10 – 2018 EY Major Technology Trends, graphically presents more details from the document.

Figure II.5. Five Major Technology Trends



Source: http://www.ey.com/gl/en/industries/financial-services/insurance/ey-tech-trends

The "Digital and omnichannel" trend relates to the fact that customers' expectations about digital and personalized access to products and services have risen dramatically with the ongoing advent of new technology and social platforms – the insurance industry needs to adapt and up its game.

"Big data and analytics" refers to the large amounts of investments the industry is undertaking to improve their modeling and data practices across the board. The "Legacy system transformation" trend, a common challenge across large corporations, is about adopting robotic process automation (RPA) software to streamline and better coordinate business processes. "Cybersecurity" is about recognizing that cybersecurity is an ongoing challenge that has to be dealt with both proactively and strategically. "InsurTech and blockchain", are new technologies that are defined as:

²⁰ coalition-against-insurance-fraud-the-state-of-insurance-fraud-technology-105976.pdf

²¹ http://www.ey.com/gl/en/industries/financial-services/insurance/ey-tech-trends

- *InsurTech* refers to the use of technology innovations designed to squeeze out savings and efficiency from the current insurance industry model²² and is the industry that's modernizing insurance with the help of wearables, the Internet of Things (IoT), SaaS applications, custom tech platforms, and more.²³ InsurTech is the insurance-specific manifestation of Financial Technology (FinTech or fintech). "InsurTechs are technology-led companies that enter the insurance sector, taking advantage of new technologies to provide coverage to a more digitally savvy customer base"²⁴.
- "A blockchain is a public register in which transactions between two users belonging to the same network are stored in a secure, verifiable and permanent way. The data relating to the exchanges are saved inside cryptographic blocks, connected in a hierarchical manner to each other. This creates an endless chain of data blocks -- hence the name blockchain -- that allows you to trace and verify all the transactions you have ever made"²⁵.

These technologies are both emerging and pervasive and result in both challenges and opportunities for collaborative approaches between software developers and traditional insurance company IT platforms.

The following section is designed to bring forward several concepts of best practices models, new and tried, for fighting fraud and cyberattacks.

THE ROLE OF SYSTEMIC ECOSYSTEM MODELS IN FIGHTING FRAUD AND CYBERATTACKS

The concept of a systemic ecosystem refers to the evident need for considering both technologies and organizational processes and structures in designing and adopting effective measures to protect data and achieve a cyber-secure environment. The quote below is from the Accenture's Technology Vision for Insurance 2017 paper²⁶:

"The biggest innovations in insurance over the next three years will not be in the technology tools themselves, but in how we design them with customers, agents, employees end other human partners in mind.

The digital revolution today is an age of human empowerment: Rapid advances have created a people-centric technology environment, where the power lies with people to shape technology as they see fit".

This over-encompassing concept, as also seen from content presented so far, is present and prevalent in best practices documents about the insurance industry and its efforts to address fraud and cyber vulnerabilities. Below, Figure II.6, shares a version of the "ecosystem" vision from the Technology Vision for Insurance 2017 research paper by Accenture.²⁷ Appendix 11, also from the report, visually shows the dynamic evolution of these drivers since 2015, and Appendix 12, contains Accenture's viewpoint on the 100 Day and 365 Days Plans to navigate the journey in the "Era of the Intelligent Insurer". These are powerful and innovative best practices.

²² https://www.investopedia.com/terms/i/insurtech.asp

²³ https://www.insureon.com/about-us/insurtech

²⁴ https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-the-threat-that-inspires

²⁵ https://www.forbes.com/sites/forbestechcouncil/2018/03/28/blockchain-what-is-it-and-what-is-it-for/#6148623a1a16

²⁶ https://www.accenture.com/us-en/insight-insurance-technology-vision-2017

²⁷ https://www.accenture.com/us-en/insight-insurance-technology-vision-2017

Figure II.6. Accenture - The Era of the Intelligent Insurer



Source: https://www.accenture.com/us-en/insight-insurance-technology-vision-2017

Having shared the valid, and aspirational, insights and program put forth by Accenture, it is important to ensure that, when thinking about implementing a new security policy, it is fully understood that there are fundamental choices and starting platforms in the current organizational realities facing insurers. Specifically, any program to address fraud abetment and cybersecurity goals needs to be considered based on two overarching realities: 1. balancing prevention with response, and 2. ensuring an integrated strategic approach. Below, we address each of these important factors.

While some of the sources are not very recent, the author puts forth that these research papers are still conceptually valid – and actionable today – as insurance companies need to shed clarity on past as well as current approaches to facing the issues at stake before engaging in advanced practices.

Again, fraud and cybersecurity programs must start with a shared and clear picture of current capabilities, frameworks and longitudinal organizational journeys.

	Features	Prevention paradigm	Response paradigm
Assumptions	Threat tempo	Information systems security threats are persistent	Information systems security threats are transient
	Control tempo	Effective information systems security controls must be persistent	Effective information systems security controls must be emergent
	Threat-control timing	Threat and control share a static relationship	Threat and control share a dynamic relationship
	Threat forecasting	Threats are predictable	Threats are unpredictable
	Threat measurement	Threats are measurable	Threats are not measurable
	Threat-control logical form	The relationship of controls to threats is determinate	The relationship of controls to threats is consequential
Logical structure	Causal structure	Variance	Process
	Unit of analysis	Variables	Events
	Safeguard-risk reduction definition	Safeguard is necessary and sufficient to reduce risk	Safeguard is part of necessary and sequence of conditions to reduce risk
	Relationship to time	Static	Dynamic
	Logical form	"If X then Y"	"If not X then not Y"
	Ideal creation	Reliability	Validity
Organizing principles	Strategic goal	Quality	Agility
	Learning strategy	Exploitation	Exploration

Table II.1. Features Distinguishing Prevention Models from Response Models

Source: R. Baskerville, P. Spagnoletti, J. Kim, *Incident-centered information security: Managing a strategic balance between prevention and response*, 2014

• Balancing prevention with response

The importance of considering balance between prevention and response is relevant for three main reasons. Firstly, companies have limited resources and budgets and, with clarity on this balance, they are better able to optimize their budgets and organizational construct interventions. Second, given the pace of change in the technology and data sets landscapes, it can be overwhelming for an insurer, or any organization, to frame a program for fraud and cyberattacks protection without specificity on the desired balance. Thirdly, and perhaps more importantly, without choices about the level of balance to be achieved – and how it might change over time – it is going to be difficult to implement the dynamic models that are necessary to flex with the shifting cyber environment. Having made the distinction between prevention and response, Table 2 below presents, from the same paper²⁸, a set of features to consider.

The authors²⁹ further delineate, in Figure II.7, the interaction between the two paradigms which is presented here to further stress the importance that key decision makers invest in understanding that, a. this "tension" exists and needs thoughtful consideration and, b. the strategy setting schematized in Figure II.7 below can be useful in continuously designing and assessing the validity of current practices.



Figure II.7. Interaction of Two Paradigms

Source: R. Baskerville, P. Spagnoletti, J. Kim, *Incident-centered information security: Managing a strategic balance between prevention and response*, 2014

· Ensuring an integrated strategic approach

An integrated strategic approach to designing a security and fraud prevention strategy is highlighted as a key element in the predominant research. Current surveys have shown that, in the insurance industry, approaches for fighting these crimes is still lacking, reactive and spotty. A recent, 2016, white paper by the Reinsurance Group of America (RGA), "Investigating Life Insurance Fraud and Abuse: Uncovering the Challenges Facing Insurers", shows that "[w]hile data and analytics were top of mind for many attendees…survey respondents indicated that 90% do not currently use algorithms to flag questionable claims or other mod-

²⁸ R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, 2014

²⁹ R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, 2014

eling methods. However, most of the respondents also indicated that they are interested in using modeling.

Needed, then, are holistic and carefully coordinated strategies that can help decision makers embrace the scope of the challenge and put in place effective programs – rather than sine points of view and function-monolithic platforms, like the ones described in Figure 17 from the paper Baskerville, R., & Dhillon, G. (2008). *Information Systems Security Strategy: A Process View*. In D. W. Straub, S. Goodman & R. Baskerville (Eds.), *Information Security: Policy, Processes, and Practices*³⁰.

Theory	Activities	Characteristics
Security policy theory	Policy establishment Policy implementation Policy maintenance	 Policy is the main focus Emphasize sequential, structured procedures
Risk management theory	Risk assessment Risk control Review and modification	 Understand and cope with insecure environments Ignore security policy and information audit mechanism Overemphasize structures
Control and auditing theory	Establish control systems Implement control systems Information auditing	 Internal control and information audit is the main focus; ignore security policy and risk management Lack of requirements planning and contingency for the unexpected
Management system theory	Establish security policy Defence security scope Risk management Implementation	 Information auditing is ignored and the implementation is affected Lack of periodic check Lack of feedback
Contingency theory	Policy strategy Risk management strategy Control and audit strategy Management system strategy	 Consider environments both outside and inside of an organization, and choose appropriate security strategies Lack of integration of structures

Table II.2. Summary of Information Security Management Theories and Characteristics

Source: R. Baskerville, G. Dhillon, *Information Systems Security Strategy: A Process View*. In D.W. Straub, S. Goodman & R. Baskerville (Eds.), *Information Security: Policy, Processes, and Practices*, 2008

Conclusion

This part of the report provided an overview of fraud and cybersecurity in the insurance industry and set forth a set of concepts and best practices to tackle the significant challenge insurers face in these domains. The author explored the current body of vast and voluminous research which reflects the ongoing and shifting issues faced by the industry. The learning from the research conducted and shared in this paper, has been presented, and is aimed at, guiding key decisions makers in insurance organizations in framing an informed conversation on how to go about implementing a best practices program for fighting fraud and cyberattacks.

³⁰ R. Baskerville, G. Dhillon, *Information Systems Security Strategy: A Process View*. In D.W. Straub, S. Goodman, R. Baskerville (Eds.), *Information Security: Policy, Processes, and Practices*, 2008

IT SOLUTIONS FOR INSURANCE MARKET

The described solutions are aimed at detection of fraudulent (here: unsubstantiated) insurance claims, and potential money laundering activities. This goal is achieved by means of the aforementioned method, with addition of scenario-based analysis (also referred to as rulebased analysis) engineered based on specifications from a particular client. These methods are used to identify not only individual criminals, but also organized crime networks.

SAS® DETECTION AND INVESTIGATION FOR INSURANCE

Description

SAS® Detection and Investigation for Insurance is a solution dedicated to determination of fraud likelihood at each step of the insurance claim process, so it provides a process innovation in fraud detection. The analytical engine of the software introduces a variety of techniques, including machine learning, rule-based approach, text mining, database searches, anomaly detection and network link analysis, to enhance the work of investigation units, fraud analysts and claims managers in insurance companies.

Manufacturer's description

Name: SAS Institute, Inc.

Description: SAS Institute is an IT company, founded in 1976, offering an advanced analytics solution for risk management, fraud prevention, customer intelligence, business analytics and data management. The headquarters are located in Cary, North Carolina, U.S., however the representative branches are dispersed all over the world, including Warsaw. The company has academic background because its foundation is a result of a project on statistical analysis led by James Goodnight, current CEO.

Expected benefits

- · Improving detection rate of fraudulent activity
- Preventing fraud losses before settlement
- Enhancement and acceleration of investigation process

Recommendations / users' opinions

User description: Allianz Insurance has operated in the insurance market since 1890. The company provides services to over 86 million clients in 70 different countries.

Benefits/opinion: "The users can browse through all of the monitored elements, which gives us a real boost in savings and efficiency" [2] – Maya Mašková, Head of the Internal Audit Department.

Measured benefits:

• 26 % more cases investigated

- 40% proven fraud cases
- Saved about CZK 110 million a year

User description: Aksigorta, founded in 1960, is a leading Turkish insurance service provider with 2,000 independent agencies, 990 branches, 69 brokers and 3,600 contracted institutions.

Benefits/opinion: "It used to take our investigators six months to expose cases of organized fraud. SAS allows us to do it in 30 seconds" [4] – Yalcin Terlemez, IT Division Manager, Aksigorta.

Measured benefits:

• Increase in fraud detection rate by 66%

User description: Alm. Brand Bank A/S, established in 1792, is a Dutch financial institution providing banking products and investment services for private customers.

Benefits/opinion: "We always presume that our customers are honest. But at the same time, we uncover fraud amounting to more than EUR 5.3 million annually" [6] – Brian Wahl Olsen, Claims Director, Alm. Brand.

User description: Sigorta Bilgi ve Gözetim Merkezi (Insurance Information and Monitoring Center) is a Turkish non-commercial institution with a legal entity, established to monitor and gather data concerning insurance services.

Benefits/opinion: "Our focus on analytics over business rules has led to the discovery of TL 259 million [US \$86 million] in potential fraud cases within the first nine months of using the solution" [8] – Aydin Satici, General Manager, SBM.

User description: Poste Assicura SpA, belonging to the Poste Italian group, is one of the largest companies on the Italian life insurance market.

Benefits/opinion: "We chose SAS because it meets our needs most effectively: easy integration with our information systems, ease of use for any skill level, and flexibility in recognizing and correlating diversified anti-fraud rules" [10] – Roberto Benassi, Portfolio and Claims Supervisor, Poste Assicura SpA.

User description: The ETHNIKI Hellenic General Insurance Company, established in 1891, is the biggest enterprise in the Greek insurance market.

Benefits/opinion: "We more than doubled our fraud savings by identifying fraudsters before claims payments were made" [12] – Heracles Daskalopoulos, Deputy General Manager, Ethniki Insurance.

Sources

- www.sas.com/en_us/software/detection-investigation-for-insurance.html
- www.sas.com/en_us/customers/allianz-fraud-management.html
- www.allianz.pl/korporacyjna/
- www.sas.com/en_us/customers/aksigorta-tr.html
- www.aksigorta.com.tr/en/hakkimizda/aksigorta-hakkinda
- www.sas.com/en_us/customers/alm-brand-dk.html
- www.bloomberg.com
- www.sas.com/en_us/customers/sbm-tr.html
- www.sbm.org.tr/en/Pages/History.aspx
- www.sas.com/en_us/customers/poste-assicura.html

- www.sas.com/en_us/customers/ethniki-insurance-gr.html
- www.igpinfo.com/igpinfo/networkpartners/publicpartners.php?greece

SAS® ANTI-MONEY LAUNDERING

Description

SAS® Anti-Money Laundering is a decision-assisting tool for anti-money laundering and counter terrorism compliance departments of insurance institutions, which is a process innovation in decision making. This solution employs risk-based approach, involving behavioural and peer-based analytics techniques for flow of fund monitoring, to improve accuracy and accelerate detection process.

Manufacturer's description

Name: SAS Institute, Inc.

Description: SAS Institute is an IT company, founded in 1976, offering an advanced analytics solution for risk management, fraud prevention, customer intelligence, business analytics and data management. The headquarters are located in Cary, North Carolina, U.S., however the representative branches are dispersed all over the world, including Warsaw. The company has academic background because its foundation is a result of a project on statistical analysis led by James Goodnight, current CEO.

Available product options

- SAS® Anti-Money Laundering [details pending]
- SAS® High-Performance Anti-Money Laundering (Distributed LASR) [details pending]
- SAS® High-Performance Anti-Money Laundering (Non-distributed LASR) [details pending]

Expected benefits

- Accelerating strategy validation by means of transparent visualization flow of funds and alert origin
- Increasing detection efficiency by higher alert quality and accuracy (improving SAR conversion up to 4 times in midsize institutions)

Recommendations / users' opinions

User description: ERGO Group is a European insurance market leader offering a wide range of insurance, provision and services.

Benefits/opinion: "With SAS Anti-Money Laundering, we save precious time and money every day" [3] – Steven Verlinden, Business Analyst.

Sources

- www.sas.com/en_us/software/anti-money-laundering.html
- www.ergo.com/en/Unternehmen/Portrait-ERGO-Group
- www.sas.com/en_us/customers/ergo-be.html

RA7

Description

The offered platform is based on Nemesysco's Layered Voice Analysis (LVA^{TM}), a technology dedicated to identification of deceptive intentions by extraction of certain vocal parameters correlated with key human emotions, which is an innovative product. This solution provides real-time insight in subject's mental state and, using signal processing algorithms, enables to detect anomalies and classify them according to a certain emotional state, such as stress, excitement or confusion. It is worth noting, that the LVA is a proprietary technology of Nemesysco and can be applied over telephone lines and standard microphones. Moreover, the core technology can be adapted to various applications, including identification of fraudulent insurance claims in real-time.

Manufacturer's description

Name: Nemesysco Ltd.

Description: Nemesysco, founded in 2000, is a provider of solutions based on voice analysis technology "Layered Voice Analysis", patented by Amir Liberman, the company's CEO, which allows personality and risk assessment. The headquarters are located in Israel, while the offered services are globally distributed by a network of partners in over 50 business locations.

Available product options

Product is available as software for analyst's computer workstation using Voice over IP interface or connected to phone via special a connector provided by Nemesysco.

Expected benefits

- Increasing fraud detection rate
- Improving customer service by shortening claims settlement time

Recommendations / users' opinions

User description: Duke University is a private institution with a long academic tradition, founded in 1838. The main campus is located in Durham, North Carolina, U.S. Duke university offers variety of highly ranked graduate programs, including Fuqua School of Business, School of Medicine and Pratt School of Engineering.

Benefits/opinion: "We find that higher levels of positive (negative) affect, as operationalized via higher levels of excitement (cognitive dissonance) determined by proprietary LVA software, convey good (bad) news about future firm performance..." [5] – William J. Mayew, Mohan Venkatachalam.

User description: University of Tsukuba is a Japanese public academic institution. The university was established in October 1973, as a result of relocation and transformation of the Tokyo University of Education. Currently, University of Tsukuba is placed on the 250th position in QS World University Ranking.

Benefits/opinion: "Psycholosoft, a research group affiliated with the Department of Psychology at Japan's Tsukuba University, determined that Nemesysco's Layered Voice Analysis (LVA) technology is a reliable and valid tool for detecting mental stress through speech" [5] – Seishin Igaku.

User description: Mamata medical college is a private medical college, founded in 1998. The main building and teaching hospital are located in the city of Khammam, Telegana, India.

Benefits/opinion: "A significant correlation was seen between the emotional factors and certain personality traits... Thus the emotions displayed through voice can be used as a tool to determine personality" [5] – Brinda Manchireddi, Josef Kamalesh, Sumaiyah Sadaf, P. Aravind Reddy.

Sources

- www.nemesysco.com/speech-analysis-technology
- http://nemesysco.com/insurance-risk-assessment-fraud-detection-ra7
- www.nemesysco.com/about-us
- www.crunchbase.com/organization/nemesysco
- · Brochures disclosed by Nemesysco staff
- · library.duke.edu/rubenstein/uarchives/history/articles/narrative-history
- www.usnews.com/best-colleges/duke-university-2920#close-modal
- · www.topuniversities.com/universities/university-tsukuba
- www.mamatamedicalcollege.com
- www.targetadmission.com/colleges/12591-mamata-medical-college-khammam

THE DEEPEYES SOLUTION

Description

The DeepEyes solution is an innovative product, artificial intelligence (AI) platform, designed to detect the emotional state of a subject through analysis of micro expressions. Real time analysis is provided by combining statistical and mathematical modelling together with machine and deep learning technologies. Relying on the data acquired by a simple HD camera, the software conduct analysis of video material and performs face recognition, as well as, emotions identification. By means of AI-assisted video processing, this solution provides emotional state truthfulness assessment, which is suitable for detecting fraudulent behaviour of insurance claimers.

Manufacturer's description

Name: DeepEyes

Description: DeepEyes is an IT solution provider for risk assessment and business analytics. The main product offered by the company is software designed to perform computer vision analysis. The company was founded in 2015 and, currently, actively operates in Germany, the Netherlands and the United Kingdom.

Available product options

Since the DeepEyes algorithm is relatively undemanding, the software can be installed on a conventional computer workstation or a mobile device equipped with an HD camera. Moreover, the software does not require an Internet connection.

Expected benefits

- · Improved fraud detection rate in the field insurance claims
- Decrease of economic losses

Sources

- www.deepeyes.co/industries/
- www.deepeyes.co/industries/financial_industry/
- www.deepeyes.co/deepeyes_team/
- www.crunchbase.com/organization/deep-eyes

RISK ASSESSMENT AT UNDERWRITING

Description

Risk Assessment at Underwriting is an innovative real time monitoring system dedicated to risk assessment in insurance industry. The offered solution is based on artificial intelligence and machine learning employed to prevent insurance fraud. The software provides insight in risk associated with application of new customers and identification of frequent claimers or high risk. With the help of AI based analysis, the system indicates groups characterized by high risk and enables identification of organized crime network.

Manufacturer's description

Name: FRISS

Description: FRISS is a European provider of analytics solutions dedicated tofraud detection, risk assessment and compliance for insurance industry. The company was founded in 2006 by Jeroen Morrenhof, its current CEO. Until now, FRISS has had two lead investors: Aquiline Technology Growth and BlackFin Capital Partners. Currently, the company's total funding amount is estimated at €15M [3].

Available product options

- Standalone Risk Assessment at Underwriting solution
- Integrated with FRISS's Compliance Screening, a solution for ensuring compliance with rules and regulations
- Integrated with FRISS's Detection at Claims, a solution for fraud detection in the field of claim process

Expected benefits

- · Improved customer experience by means of automated verification process
- · Balancing quality and quantity of portfolio growth by detecting high-risk clients
- Improved fraud prevention
- Application of an integrated solution provides fraud prevention during both new customer application as well as claim process and ensures compliance with law regulations

Recommendations / users' opinions

User description: SIGNAL IDUNA group is one of the largest insurance companies in the German market. Currently, the company is expanding into foreign markets, including Poland, Hungary, Romania and Switzerland.

Benefits/opinion: "By choosing FRISS we have found the best possible solution available in the market" [6, 8].

User description: Folksam, founded in 1908, is a leader in the Swedish market of non-life insurance products. In 1925, the company expanded onto the Finish insurance market.

Benefits/opinion: "Folksam has chosen FRISS as we see that the FRISS platform is built and designed for the needs of the insurance business" [6, 11].

User description: InShared is an internet insurance company established in 2009 as an initiative of Eureko – Achmea, one of the largest insurance companies in the Netherlands. The first company which guarantees refunding of surplus profits to its clients.

Benefits/opinion: "With the help of FRISS we managed to retain 6% premium, which is refunded to the customers who have not submitted claims" [6, 13].

User description: Reaal is a Dutch insurance company and a part of the SNS Reaal group.

Benefits/opinion: "With FRISS we proactively estimate risk. This enables us to stop potential fraudsters before they enter our portfolio" [6, 14].

User description: Malta insurance association (MIA) is a non-profit institution uniting all insurance companies in Malta, including foreign investors. The association represents common interest of its members and its current efforts are dedicated to fraud prevention and procedures associated with traffic accidents.

Benefits/opinion: "Having a number of insurers bundling their potential means a lot to us and the FRISS country platform makes this possible" [6, 16].

User description: INTERAMERICAN, currently belonging to the Achmea group, is a leader in the Greek private insurance market. The company now operates in all insurance branches and has over 1M of individual and corporate clients.

Benefits/opinion: "Our target is to make sure that high risk and fraud cannot enter our books. We want to have an integrated solution both for motor underwriting and claims, based on user friendly technology" [6, 18].

Sources

- FRISS, Risk Assessment at Underwriting product sheet
- www.friss.com/en/solutions/risk-assessment-at-underwriting/
- · www.crunchbase.com/organization/friss
- www.friss.com/en/solutions/fraud-detection-at-claims/
- www.friss.com/en/#row-solutions
- www.friss.com/en/
- www.signal-iduna.pl/signaliduna/o-nas
- · www.friss.com/en/our-work/signal-iduna/
- www.folksam.fi/vakuutusyhtio-folksam/about-folksam-english
- www.crunchbase.com/organization/folksam
- www.friss.com/en/our-work/folksam/
- pl.linkedin.com/company/inshared
- www.friss.com/en/our-work/inshared/
- www.friss.com/en/our-work/reaal/
- www.maltainsurance.org/about-us/
- www.friss.com/en/our-work/malta-insurance-association/
- www.interamerican.gr/default.asp?pid=2&la=2
- www.friss.com/en/our-work/customer-story-interamerican/

ARIC PLATFORM

Description

The proposed software platform offers real-time monitoring and analysis of customer data to detect and prevent fraud by detecting behavioural anomalies, which is a process innovation in crime detection in the insurance industries.

The embedded adaptive behavioural analytics module is based on machine learning and statistical modelling, which introduce a self-learning mechanism and allow to reduce manual intervention. The software builds a behavioural profile for each individual user based on the data acquired by Javascript and Mobile SDK collectors. The manufacturer offers PCI-DSS certified environment for securing customer data. The data interface is provided by means of a dedicated RESTful API available through http and https protocols. The applications of the software in question encompass detecting insurance application fraud.

Manufacturer's description

Name: FeatureSpace

Description: FeatureSpace Limited was founded in 2005 by David Excell, currently Chief Technology Officer and Director, and his PhD supervisor, Bill Fitzgerald, a Cambridge Uni-

versity Professor. The main product of the manufacturer is a software platform dedicated to fraud prevention based on behavioural analytics. The company's headquarters are located in Cambridge, UK, and Atlanta, GA, U.S. In 2018, the company was awarded for its Anti-fraud Solution of the Year at FStech Awards.

Available product options

- Software installation on customer's IT infrastructure
- Access to software via a secure web connection

Expected benefits

- Real-time identification of insurance application fraud
- Reduction in the number of manual interventions resulting in improving operational efficiency up to 50%
- Reducing the number of false positive alerts by up to 70%
- · Improving customer experience by reducing unnecessary interruptions

Sources

- www.featurespace.com/products/
- www.bloomberg.com
- www.crunchbase.com

ENERGY MARKET

EXAMPLES OF INCIDENTS OF SECTOR-SPECIFIC CYBERATTACKS AND FRAUD IN THE ENERGY SECTOR

Typically, and predominantly, the Energy sector experiences cyberattacks because of its critical infrastructure role in driving the welfare of the economy of a country – the attacks are often politically motivated. This sector has been experiencing ever increasing and severe cyberattacks.

Unlike financial institutions, who have been fighting these attacks through advanced technologies and innovative approaches, in the experience of the authors, few, if any, energy companies are functionally structured – or have the technical capability in their IT or Compliance function – to fend off hostile access to their systems. The role of regulating agencies and collaborative approaches is especially important for this sector.

 Energy Firms Are Worried About Cyber Attacks, But Don't Really Know What To Do. Forbes, March 7, 2018¹

"The energy industry was relatively late to adopt digitalization, even though – as an asset-intensive sector with many remote and hazardous sites – it is in many ways the ideal setting for the industrial internet of things. In part this was because of the importance of energy infrastructure to national economies and companies' subsequent caution about adopting new technologies. There was also a certain amount of complacency because until recently, most energy installations "did not communicate with traditional IT networks," according to Greentech Media². However, the growing complexity and decentralization of the grid, the growth of renewable energy and the increased availability of technologies such as sensors, machine learning and big data, have started to make their mark. As the vehicle sector also becomes more electric and the automotive and energy sectors become more integrated, this trend will only increase. "As the energy sector systems that monitor and run operations become more interconnected from smart grids, smart devices, and the growing internet of things, it increases the risk that a cyberattack could result in physical damage," Marsh said.

¹ https://www.forbes.com/sites/mikescott/2018/03/07/energy-industry-worried-about-cyberattacks-but-doesnt-reallyknow-what-to-do/#774f405a68bb

² https://www.greentechmedia.com/articles/read/energy-sector-ups-cyber-security-amid-growing-it-threats#gs. OXgDL6U

Cybersecurity Bill: Vital Need Or Just More Rules? US National Public Radio, March 22, 2012

"Consider what Hurricane Katrina did to New Orleans, and you get an idea of the consequences of a cyberattack on critical U.S. infrastructure: No electricity. No water. No transportation. Terrorists or enemy adversaries with computer skills could conceivably take down a power grid, a nuclear station, a water treatment center or a chemical manufacturing plant.... The prospect of such a paralyzing strike has convinced U.S. security officials and members of Congress that a new law may be needed to promote improved cyberdefenses at critical facilities around the country"³.

• New cyber resilience report: energy sector prime target for cyberattacks. World Energy Council, 2017

"Addressing cyber risks in the energy sector is critical not only to energy security, but is also vital for a resilient state and economy; finds a new World Energy Council report. The report highlights that energy companies have seen a massive increase in the number of successful cyberattacks over the past year"⁴.

INDUSTRIAL CONTROL SYSTEMS

Industrial control systems (ICS) are computerized automation systems used in physical operations and processes in various industry sectors such as electric power generation and distribution, oil and natural gas production, refining, and distribution, drinking water and wastewater treatment and distribution, manufacturing, chemical plants, and transportation (railways). The ICS umbrella category includes SCADA systems, which tend to be used in remote control operations over large distances such as for pipelines, and distributed control systems (DCS), which tend to be used in geographically closer settings such as refineries and plants.

Most of the industry sectors that use and depend on ICS are so-called critical infrastructure sectors, which deliver products and services that are essential to the wellbeing of modern society. Because critical infrastructure sectors are highly dependent on computer systems and communication and thereby potentially vulnerable to electronic attacks, cybersecurity is a topic of critical importance. ICS face cybersecurity challenges that are similar to those that general IT systems face, but ICS are different from general IT systems in the possible consequences of attacks, system requirements (especially with respect to availability), and which part of the organization is responsible for the management of the systems.

Consequences of Attacks on Control Systems

The most dramatic difference between ICS and general IT systems consists of the possible consequences that could result from a cyberattack. In general with IT systems, data can be stolen or manipulated and services can be disrupted, and while the damage can be substantial, the nature of the damage is limited to financial losses. In ICS, on the other hand, cyberattacks could have severe consequences not only financially but also in terms of human

³ https://www.npr.org/2012/03/22/149099866/cybersecurity-bill-vital-need-or-just-more-rules

⁴ https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-forcyberattacks/

health and safety, the environment, and the stability of society. Imagine that an attacker gains administrative privileges on a system that controls a critical process such as an electric power grid, a pipeline that delivers heating fuel to a large city in the winter, a petrochemical plant, or a water treatment plant. The attacker could cause denial of service by shutting down the processes, or other damage by manipulating the process to cause dangerous physical conditions.

For example, the massive blackout in the northeast United States in 2003 has been cited as a possible estimate of the potential of a well-crafted and timed cyberattack. The "Aurora" study by the US Department of Homeland Security in 2007 validated the possibility of a remote cyberattack damaging motors and generators that would require months, or longer, to repair or replace. Untargeted attacks that have affected critical infrastructure systems, such as the result of malicious software infections by common worm or virus infection have resulted in the forced shutdown of electric power generation plants and municipal air traffic systems. A teenager in Ludz, Poland was able to override control of the local tram using an infrared television remote control, causing damage to the system. The recent "Flame" malware attack against the oil conglomerate Saudi Aramco damaged a reported 30,000 computer workstations, although the control systems were not damaged.

Using systems for drinking water and wastewater as examples, one could imagine many actions that a malicious attacker could take. An attacker who takes control of an ICS for drinking water treatment or delivery could disrupt the flow of drinking water to customers, could cause overdosage or underdosage of disinfectant (both potentially dangerous to customers), or manipulate pH levels of the drinking water to cause long-term problems. In a wastewater management system, an attacker could reverse flows, or cause release of untreated sewage. It should be noted that such scenarios are not imaginary – in fact, the wastewater scenario has already happened. Lastly, Stuxnet is a case of one successful, deliberate attack that destroyed about 1,000 IR-1 centrifuges out of about 9,000 deployed at a site in the Middle East. Stuxnet was unlike any other virus. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.

Attack Case Study - Maroochy Water Services Australia

In the year 2000, a wastewater system operated by Maroochy Water Services in Maroochy Shire, Queensland, Australia, was attacked by a person who was a former employee of its system vendor. The attacker was an insider in the sense that he had intimate inside knowledge of the system, even if he was not an employee of the attacked organization. This incident is important to study because it is described in detail in a public record, and it was an intentional, targeted attack by a knowledgeable person (an insider) on an industrial control system.

In brief summary, the attacker used stolen radio equipment to access the system, and his actions caused 800,000 liters of raw sewage to spill out into local parks, rivers, and even the grounds of a Hyatt Regency hotel. "Marine life died, the creek water turned black and the stench was unbearable for residents," said a representative of the Australian Environmental Protection Agency. The attack illustrated several key vulnerabilities and attack vectors of ICS, including:

- · Unprotected access to wireless communications
- · Common radio equipment able to spoof control devices
- Devices connected to the control network without authentication

- Minimal control of user accounts and access
- Insiders with knowledge of system operations and vulnerabilities

The Maroochy incident teaches us valuable lessons about security controls that were missing from the targeted system, and how such security controls can prevent similar incidents from happening.

Attacker Categories for ICS

Several categories of threat agents could pose security threats to ICS. The listing of categories in Table III.1. Attacker Categories for ICS is based on a similar listing in NIST Special Publication 800-82⁵.

Table III.1. Attacker	Categories for ICS

Threat Agent	Description
Novice hackers	ICS make a tempting target for individuals experimenting in identifying and exploiting computer system vulnerabilities. Many inexperienced hackers (script kiddies) discover ICS systems by accident, without the background knowledge to directly attack or control the ICS system, but can still inflict inadvertent damage. New systems such as Shodan that have pre-identified vulnerable ICS systems worldwide make the novice hackers task much easier.
Black hat hackers	So-called black hat hackers break into networks for the thrill of the challenge or for bragging rights in their community. While remote cracking once required a fair amount of skill or computer knowledge, relatively unskilled attackers, known as script kiddies, can now download attack scripts and protocols from the Internet and launch them against victim sites.
Bot-network operators	Bot-network operators are attackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of compromised systems and networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or the use of servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. Some criminal groups may try to extort money from an organization by threatening a cyberattack. At a 2007 SANS SCADA conference, a representative from the U.S. intelligence community reported that several non-U.S. electric utilities had been the target of extortion attempts.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power. Along with the attack against Saudi Aramco mentioned earlier, recent cyberattacks against ATM machines in South Korea and banks in the US are the latest example of purported nation state attacks against critical infrastructures. Cyberattacks against Estonia during its dispute with Russia showed that nations are beginning to understand how to employ cyber-based methods in conflict situations.

⁵ https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Insiders	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners. Unintentional impacts from insiders are some of the highest probability occurrences.
Phishers	Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organizations that distribute unsolicited e-mail with hid- den or false information to sell products, conduct phishing schemes, distribute spyware/ malware, or attack organizations (e.g., DoS).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Malware is getting more advanced and there have been examples of malware targeting specific organizations and systems.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information. Terrorists may attack one target to divert attention or resources from other targets. Although the motives and targets of terrorist organizations trend towards more "sensational" acts, there is a growing fear that as knowledge and ca- pability for cyberattacks grows, terrorist groups may begin to use cyber methods to impact targets to illustrate their growing capability and draw attention to their causes.
Industrial/ economic spies	Industrial or economic espionage seeks to acquire intellectual property and know-how by clandestine methods. There have been many reports of large-scale long-term economic espionage successfully conducted through cyberattacks.
Social Hackers ("Hacktivists")	Social activist groups such as "Anonymous" have gained notoriety for their continued efforts at attacking a variety of individuals, corporations, and infrastructures. These groups have a range of members with significant capabilities to disrupt ICS operations, and are often unpredictable in their choice of targets.

Potential Threat Scenarios in ICS

To fully understand the importance of cybersecurity for ICS, it helps to consider some possible incident scenarios. The following are hypothetical but plausible relating to the earlier discussion of consequences of attacks:

- Control systems operation disrupted by delaying or blocking the flow of information through corporate or control networks, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-related services (such as DNS).
- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCA-DA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment.

- False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Control system software or configuration settings modified, producing unpredictable results.
- Safety systems operation interfered with, so that the safety system is no longer able to safely shut down the process when parameters reach dangerous levels.
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system, directly via the network or through the use of removable media such as a USB stick.
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.
- Physical breach at a remote site such as a pipeline compressor station or water pump facility, allowing the intruder to establish a connection back to the control network.

Security Controls for ICS

Security controls are defined as the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information. NIST Special Publication 800-82 lists general security controls together with specific recommendations and guidance for ICS for each category of security controls, too extensive to summarize here. Those security controls along with the ICS-specific adaptations form the basis for the security analysis in the remainder of this document.

Security controls for ICS are similar to those of traditional enterprise IT systems, but their deployment and operation need to be tailored to the unique operating and security needs of the industrial environment. For example, although patch management has become an almost continuous process in IT environments, in ICS environments patching may be able to be accomplished only during annual maintenance windows – alternative controls need to be implemented to mitigate vulnerabilities in unpatched systems. The following sections describe the challenges faced in implementing typical cybersecurity controls in an ICS environment.

Security Control	Description	
Personnel Security	It is a common practice for the ICS environment to have policies and procedures in place for personnel position categorization, screening, transfer, penalty and termination. This relates closely to the need of human safety in the ICS environment more than in the IT environment; hence, the screening of the personnel becomes imperative.	
System and Services Acquisitions	An ICS organization should engage with external suppliers with the same policies and procedures to maintain the overall level of ICS security. In the U.S., there is a procurement language for specifying security policies and procedures when procuring new systems.	
Awareness and Training	These are security controls implemented and executed primarily by people to ensure that the personnel receives the appropriate security training relative to their use of the system. They directly relate to the ICS needs for human safety and for reactive mechanisms in case of an emergency.	

Table III.2. Security Controls for ICS

Event Monitoring and Logging/ Auditing	Logging and analyzing system, network, and application events is a critical element in identifying unauthorized actions and events on the ICS, but the limited logging and storage capabilities of ICS devices render useful analysis difficult. New processes are being developed to correlate events from different devices to identify malicious activity.
Contingency Planning	The contingency plans should cover the full range of failures that are caused by security or failure events. They should specify roles and responsibilities, assigning personnel and activities for restoring the system after failure or attacks. This critical need for ICS systems is more complex than in the case of IT systems, involving both physical and cyber systems.
Incident Response	An incident response plan is required in the ICS environment to rapidly detect incidents and minimize their effects. The plan is more complex compared to the IT systems, because it has to cope with the availability requirements exhibited by ICS systems.
Strong Authentication	Complex passwords, password change periods, biometrics, and two-factor authentica- tion methods are becoming more the norm in enterprise IT environments. The complexity of some of these methods may induce login errors for operators in high-stress situations, or (in the case of biometric scanners) are inoperable in situations where safety clothing must be worn.
Account Management	It is common practice for ICS environments to have a single user account for access to systems and processes. This stems from the need to keep programs and processes running continually; there is a fear that log off and log on sequences might disrupt operations, particularly if a safety or security incident occurred, or was forced by an attacker, during the log in period.
Access Control / Least Privilege	Limiting the authority of user accounts to perform certain dangerous or critical activi- ties, such as changing safety settings or modifying processes, are standard IT practices that could limit an operator's ability to respond rapidly in emergency situations.
Patch Management	As mentioned earlier, enterprise IT environments routinely perform weekly (or more frequent) network, system, or application updates, either to add new features or mitigate new vulnerabilities. The limited maintenance windows afforded ICS environments means that alternate means of mitigating system or application vulnerabilities must be developed and deployed.
Anti-Virus Software	Similar to patch management, the ability to download and install daily virus signature files is not always present in ICS environments that may be physically isolated; also, there is some risk (and ample evidence) that installing new anti-virus signatures might impact legitimate system application.
Intrusion Detection Systems (IDS)	Although common in business IT environments, IDSs for control system environments are only beginning to be deployed. Enterprise IT IDS systems are not geared for industrial environments or protocols, and have a false alarm rate that is resource intensive to resolve. Intrusion Prevention Systems (IPS) that can reconfigure network ports and protocols based on IDS activity are highly problematic for ICS environments where a false positive may incorrectly shut down critical processes.

IT SOLUTIONS FOR ENERGY MARKET

This part of report summarizes an analysis of available fraud detection/prevention IT solutions performed by the authors.

IIC SOLUTION FOR ENERGY FRAUD DETECTION

Description

The offered services are applicable in various types of energy distribution, such as gas or electricity. The identification of frauds and irregularities is based on predictive models and statistical techniques for determination of correlations and relations among clients. Further steps of evaluation involve use of classification techniques, supported by historical data concerning clients' behaviour, to estimate probability of fraudulent behaviour of each individual client.

Manufacturer's description

Name: IIC (instituto de ingenieria del conocimiento)

Description: IIC is a private institution founded in 1989 by the Asociación para el Desarrollo de la Ingeniería del Conocimiento (ADIC), an association of academic and business partners, including Banco Español de Crédito, Banco Hispano Americano, Iberia, El Corte Inglés IT, INH-Repsol, IBM, RENFE, Tabacalera, Unión Eléctrica Fenosa and Universidad Autónoma de Madrid. Currently, Instituto de ingenieria del conocimiento focuses on providing solutions for extraction of useful data based on voluminous collection (big-data) in various areas, including banking, healthcare, social media, energy and human resources.

Sources

- http://www.iic.uam.es/en/big-data-services/energy-environment/energy-fraud-detection/
- http://www.iic.uam.es/en/iic-about/who-are-we/

SHAPE

Description

SHAPE is an innovative analytics platform dedicated to customer profiling and fraud detection in the energy industry. This solution is a direct result of collaboration between Enel (energy company), Politecnico do Torino (scientific partner) and Exueura (industrial partner) and provides a web-based platform enabling:

- · Identifying customers' consumption/production profiles
- Forecasting customers' energy consumption with 15 minutes resolution

- Simulating energy distribution based on different real and assumed pricing plans
- Predicting possible fraudulent activities

Manufacturer's description

Name: Exeura

Description: Exeura s.r.l. was founded in 2000 as a research spin-off from the University of Calabria, Italy. The company still maintains connections with academics as the president of Exeura, Pasquale Rullo, is a professor at University of Calabria. Exeura provides business analytics solutions based on exploring and processing voluminous sets of data.

Expected benefits

- Insight in energy consumption/production patterns
- Increased effectiveness of energy distribution
- · Reduction of economic losses caused by anomalies and fraudulent activities

Recommendations / users' opinions

User description: Enel is a multinational energy company, currently operating in 35 countries and having 63.5 million end users around the world.

Benefits/opinion:

- Improvement of pricing schemes
- Decrease in investment costs by reducing the planning margin
- Energy fraud detection
- Increased effectiveness of energy management

Sources

- www.exeura.eu/en/solution/public-utility/
- http://www.exeura.eu/en/exeura/about-us/
- www.enel.com/aboutus/who-we-are

SAS[®] ENTERPRISE MINER[™]

Description

The offered software is developed to assist analysts in decision-making process by creating reliable predictive and descriptive analytical models, which makes the decision-making process more innovative and efficient. The analysis is performed by employing data mining to extract relationships and answers from large sets of data composed of call center logs, survey results, customer feedback forms, web data and time series data.

SAS® Enterprise Miner[™] can be applied in the energy industry as a useful tool in energy fraud detection and estimation of resource demands.

Manufacturer's description

Name: SAS Institute

Description: SAS Institute is an IT company, founded in 1976, offering an advanced analytics solution for risk management, fraud prevention, customer intelligence, business analytics and data management. The headquarters are located int Cary, North Carolina, U.S., however the representative branches are dispersed all over the world, including Warsaw. The company has academic background because its foundation is a result of a project on statistical analysis led by James Goodnight, current CEO.

Expected benefits

- Identifying technical and nontechnical causes of economic loss
- Increasing efficiency of fraud detection
- Reducing economic losses caused by abnormalities and frauds

Recommendations / users' opinions

User description: Cemig is one of the biggest electric energy provider in Brazil and a power generator with capacity of 7,295 MW.

Benefits/opinion:

- Detecting abnormalities in energy usage, including technical faults in meters and energy deviations
- Detecting over half of energy frauds committed
- Preventing economic losses amounting to \$420,000 per month

Sources

- www.sas.com/en_us/software/enterprise-miner.html
- www.sas.com/en_us/customers/cemig-br.html

VITRIA OPERATIONAL INTELLIGENCE (OI)

Description

The offered software provides real-time analytics of streaming data from smart grid network, smart meters, sensors, as well as web content, including weather and traffic information and social media. Using state-of-the-art streaming processing techniques, Vitria OI enables energy firms to obtain real-time insight in the grid activity and support to take immediate action based on insight in the grid activity visualized by means of dashboards. In particular, the behavioural-based detection allows to identify energy reversal or voltage fluctuations, but also to correlate it with user information and send real-time notifications of potential fraud to authorized personnel.

Manufacturer's description

Name: Vitria Technology, Inc.

Description: Vitria Technology, Inc., established in 1994, is a company offering solutions for Internet of Things (IoT) and operational intelligence (IO), suitable for Energy, Telecommunications and Manufacturing. The firm has achievements, documented by patents and awards, in field of streaming technology suited for business process management. Currently, Vitria operates in North and Latin America, as well as in Asia.

Expected benefits

- Energy theft detection & smart grid security
- Monitoring and management of energy demand
- · Preventive infrastructure maintenance based on real-time performance monitoring
- Billing and provision in real-time

Recommendations / users' opinions

User description: A European gas and electricity carrier operating in over 200 cities and having over 4,000 employees.

Benefits/opinion: "We needed a robust enterprise-level solution for smart meter analysis and management. The system is needed to manage events and alarms, and also to integrate with many legacy and business process management systems. Vitria had the only solution that met these challenging requirements for managing and analysing the 4M+ meters in our network" [2].

Sources

- Vitra, Whitepaper on 5 Ways Energy & Utilities Firms Can Capitalize On Streaming Analytics, available at: www.vitria.com/pdf/WP-Energy-041514.pdf?submissionGuid =74a13d39-ea57-4ede-834d-00a4b85f9913
- Vitria, Vitria IoT Analytics Platform for Smart Meter Management Case Study, available at: www.vitria.com/wp-content/uploads/2015/08/Smart-Meter-Management.pdf

Utilization of new technologies in the energy sector

In this part of the report we aimed to provide an overview of cybersecurity and fraud challenges in the energy sector.

Concluding the considerations, it is also worth mentioning that the energy sector primarily employs big data analytics based on frequent read-outs from consumer meters (e.g. electricity, natural gas, etc.) to detect abnormalities in energy use with respect to the typical pattern of a particular user or a group of users. The collection of those technical and analytical means of analysis is called the smart-grid.

The data collected in this way are also successfully employed in improving the pricing schemes and energy management (prediction of supply/demand) of energy providers.

MANAGING PEOPLE

COMPLIANCE

Introduction

The study you are about to read explains how compliance faces the main existing problems in managing people in organizations. Companies have been dealing with problems such as violence, harassment and discrimination for many years, however, the number of complaints has lately raised considerably. Observing these events, national legal policies and international law have adapted to fight against these issues. Building on this context, the need for enterprises to follow the legislation has become a reality, making compliance an essential tool for sustainable and ethical companies.

Identification problems inside the organization

The problems one can find at the workplace are very complex and can be manifested in many different forms. We can divide them in three blocks: physical violence, psychological violence, including sexual harassment, bullying and mobbing, and discrimination.

Even if workplaces should represent violence-free environments where one can find space for dialogue and debate, it turns out that employees, at any level of the hierarchy scale, often confront personal and professional problems. Thus, relationships between workers, managers, clients or the public deteriorate, and the objectives of working efficiently and achieving productive results are negatively affected. When this situation occurs, the workplace becomes a hostile environment where people cannot properly develop professionally.

Being in such situations may result in anxieties and frustration of employees, organizational and production difficulties, personality clashes, diminished resources, decreasing production or output demands, aggressive intruders, and problematic relations with clients and the public. In order to solve them, it is important to understand each of the complications that may emerge¹.

Due to the increasing relevance of this topic, there has been a general shift on the number of offences against the rights of people in paid work registered in the courts. The evolution in

¹ D. Chappell, V. Di Martino, *Violence at work. International Labour Organization*, 2006, http://www.ilo.org/ wcmsp5/groups/public/%40dgreports/%40dcomm/%40publ/documents/publication/wcms_publ_9221108406_en.pdf

Poland is displayed in Figure IV.1. The higher decrease has been in the malicious infringement of rights². The data from Polish courts also brings evidence on the type of crimes that are most frequently committed. These can be found in Figure IV.2. Compensation for violation of the principle of equal treatment in employment and compensation in connection with mobbing / workplace harassment / workplace bullying are the two crimes that are reported with the higher number of cases. Nevertheless, as shown in Figure IV.3, only the 12% and the 11% of them were included, respectively. In contrast, although compensation for sexual harassment gets the fewer cases, it turns out to be the type of crime with the higher rate of inclusion.



Figure IV.1. Offences Against the Rights of People in Paid Work in Poland

Source: Ministry of Justice of Poland

Figure IV.2. Records of cases related to discrimination in Polish Regional Courts: Total resolving in 2016/17



compensation for violation of the principle of equal treatment in employment

compensation in connection with mobbing / workplace harrassment / workplace bullying

discrimination in employment

compensation for sexual harassment as one of the forms of discrimination at work

Source: Ministry of Justice of Poland

² Art. 218. Malicious infringement of rights:

^{§ 1.} Anyone who, while performing labour law and social insurance activities, maliciously or persistently infringes the rights of employee under an employment or social insurance relationship is liable to a fine, the restriction of liberty or imprisonment for up to two years.

^{§ 2.} If person specified in § 1 refuses to reinstate a person despite being ordered to do so by the appropriate authority, he or she is liable to a fine, the restriction of liberty or imprisonment for up to one year.

^{§ 3.} If person specified in § 1 fails to comply with a court judgment ordering that remuneration be paid or another allowance be given under an employment relationship, he or she is liable to a fine, the restriction of liberty or imprisonment for up to three years.


Figure IV.3. Percent included from the total resolving in 2016/17

Source: Ministry of Justice of Poland

Preventing violence, bullying and harassment at the workplace

Physical violence and at the workplace

Violence, is "any action, incident or behavior that departs from reasonable conduct in which a person is assaulted, threatened, harmed, injured in the course of, or as a direct result of, his or her work:

• Internal workplace violence is that which takes place between workers, including managers and supervisors.

• External workplace violence is that which takes place between workers (and managers and supervisors) and any other person present at the workplace."³

Table IV.1. What Constitutes Physical Violence

The examples of violent behaviors at work can be listed as follows: homicide, rape, robbery, victimizing, wounding, intimidation, battering, threats, physical attacks, kicking, biting, aggressive posturing, punching, spitting, interfering with work tools and equipment, throwing objects, scratching, hostile behavior, squeezing, pinching and related actions, swearing, shouting, stalking, name-calling, including sexual and racial abuse, innuendo.

Source: Chappell, D. and Di Martino, V., 2006. Violence at work. International Labour Organization

Table IV.2. Experiences of Physical Violence - example

United Kingdom

The 2016/17 Crime Survey for England and Wales (CSEW) estimated that 1.3% of the people in the working age had suffered from violence at work; 0.5% had suffered from physical assaults. Figure IV.4 presents the statistics mentioned⁴. The distribution of different incidents resulting from violence at the workplace are displayed in graph 2, showing that the vast majority of people who experienced such situations, do not end up injured. From those injured, the most common problem was minor bruising or black eye.

³ ILO, 2004b, p. 4

⁴ http://www.hse.gov.uk/statistics/causinj/violence/work-related-violence-report-2018.pdf







Figure IV.5. Percentage of violence at work incidents by injury type 2016/17 (CSEW)

Psychological Violence

Psychological violence "can include diverse aggressive tactics, all of which have the potential to cause significant emotional injury among those victimized. It is often considered to include bullying, mobbing, coercion, verbal abuse and sexual harassment, hostile behavior, leaving offensive messages, swearing, shouting, stalking, deliberate silence, innuendo, rude gestures,. Many of these forms of workplace violence are repeated by the perpetrators and while one-off events may be relatively minor, the cumulative impact on the recipients results in very serious consequences (often with a greater impact than that from physical violence), for example following repeated acts of sexual harassment, bullying or mobbing."

Traditionally, the focus has been on physical violence, mainly due to its visibility. Nevertheless, in recent years the relevance and evidence on non-physical violence has increased. The impact and harm on a daily basis of the employees has become a worldwide burden. Many enterprises around the world have reported such behaviors and so have done the courts.

 Table IV.3. Deadly Consequences of Psychological Violence

Suicide is responsible for nearly 1 million deaths worldwide each year, and the rate is continuing to rise — particularly in the workplace, according to a new study [3]. Researchers have linked these suicides to a generalized deterioration of working conditions, including unmanageable workloads and increased job insecurity.

Source: Crime Survey for England and Wales for year ended March 2017

Workplace suicide remains a largely hidden phenomenon in most countries, and is unrecognized in legislation, absent from official statistics, overlooked by the authorities and widely misunderstood.

In most countries work-related suicides are not officially monitored or recorded. In the absence of official data or evidence, public authorities and employers tend to overlook the phenomenon.

Deadly increase: some evidence in the UK

A 2017 report by the UK government's National Suicide Prevention Strategy Advisory Group showed that suicide rates in England increased since 2007. Certain occupational groups are exposed to higher risk: including doctors, nurses, veterinary workers, farmers and agricultural workers.

Deadly evidence: the case of orange in France

In France it was the impact of stress at work was made brutally clear by a wave of suicides at French telecoms giant Orange between 2008 and 2009. In that period, 35 employees took their lives, some of them in the workplace itself. Many of them left suicide notes blaming their "terror" of management and the shock of being shunted from one job to another with no regard for their skills.

One man jumped off a bridge after being transferred to a call center. A 32-year-old woman threw herself out of an office window just days after a technician tried to commit suicide by stabbing himself in the stomach during a meeting when he learnt his job was being scrapped.

The former boss of France Telecom, Didier Lombard, and the company were charged with harassment in July 2012 - a first in France.

Karoshi (i.e. death from overwork): the case of Japan

In 2014, Japan's parliament passed a law against *karoshi*, that is, death from overwork. In Japan, more than 2000 applications for workers' compensation or survivors' benefits are filed annually by workers or families seeking state recognition for death, disability or depression caused by overwork. It is estimated that in the country there are 8000 work-related suicides (out of 30.000 total suicides). The true toll is probably much higher, since 10 percent of the male labor force work 60-plus-hour weeks under the same conditions as those who die or become mentally unstable. There are more than 10,000 non-suicide *karoshi* deaths each year.

Dangerous professions for men and women

The ONS suicide prevalence statistics for 2011 to 2015 confirmed for women, occupations with a high risk of suicide include nurses (23 per cent above the national average), primary school teachers (42 per cent above average) and those working in culture, media and sport (69 per cent above average).

The United States: third leading cause of occupational death

The US Department of Labor declared that, in 2015, 417 workplace homicides took place. Eighty-five percent of the victims were men, 356 were homicides to men and 61 were homicides to women. Homicides represented 18 percent of fatal occupational injuries to women in 2015 compared with 8 percent of fatal occupational injuries to men⁵.

⁵ https://www.bls.gov/iif/oshwc/cfoi/workplace-homicides.htm

Sexual Harassment

Sexual harassment is "any form of unwanted verbal, nonverbal or physical conduct of a sexual nature occurs, with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment." ⁶

This type of violence can be found in different manners depending on the features of its behaviors or types of communication.

Table IV.4. Definition and Types of Sexual Harassment

On its physical form, this type of violence is deliberate and unsolicited physical contact; unnecessarily close physical proximity; and stalking, for example, repeatedly following in an insistent but often unobtrusive way.

Verbal harassment consists of repeated sexually oriented comments or gestures about a person's body, appearance or life-style; offensive phone calls; questions or insinuations about a person's private life; sexually explicit jokes or propositions; persistent invitations to social activities after a person has made it clear they are not welcome; unwanted compliments with sexual content; sexually coloured remarks, bantering or innuendo; name-calling; playing games with a person's name; and reference to sexual orientation.

Adopting a coercive behavior to influence or affect, in any manner, a person's job, career or status, or an explicit/implicit promise of career advancement in exchange of sexual favours; explicit/implicit promise of recruitment in exchange of sexual favours; threatening of dismissal if sexual favours are not granted; and making work difficult if sexual favours are not granted.

Showing or displaying sexually explicit graphics, cartoons, pictures, photographs or Internet images. Doing offensive jokes of a sexual nature; display of pornographic material, graffiti, pin-ups etc.; exposure of intimate parts of the body; and use of obscene language would result in creating a hostile environment.

Repeated sexually oriented gestures about a person's body, appearance or life-style; nods, winks, gestures with the hands, fingers, legs or arms, signs and other offensive behaviour which is sexually suggestive; and persistent leering at the person or at part of his/her body. Offensive, letters or e-mail messages constitute written harassment.⁷

The current study used an experience sampling method (ESM) that captures a within-person approach to determine how the intensity of sexual harassment incidents affects the appraisal of fear of retaliation and perceived distress, which then influence organizational blame for sexual harassment across multiple experiences of sexual harassment.⁸

Source: Di Martino, 2002a; Madera, 2018.

⁶ Extract from the European Directive 2002/73/EC.Source: European Parliament, 2002a. Similar definitions of sexual harassment can be found: R.K. Jacobson; A.A. Eaton, *How Organizational Policies Influence By-stander Likelihood of Reporting Moderate and Severe Sexual Harassment at Work*, "Employee Responsibilities & Rights Journal", March 2018, Vol. 30 Issue 1, p. 37-62

⁷ ILO, 2004b, p.a.

⁸ J.M. Madera, When Targets Blame Their Organization for Sexual Harassment: A Multilevel Investigation of Within-Person Appraisals, "Cornell Hospitality Quarterly", February 2018, Vol. 59 Issue 1, p. 49-60

Bullying

"Workplace bullying refers to unwanted negative behavior (verbal or nonverbal), actions, and incidents that occur repeatedly and frequently (e.g., weekly) and over a period of time (e.g., for about six months) and that may potentially cause discomfort on a psychological, emotional, and/or physical level. Bullying behavior includes acts of harassment that offends, socially excludes, or negatively affects a person's work⁹". The bullying behavior may also manifest in physical or unspoken threats, coercion, intimidation, embarrassment, sabotage, or the disruption of productivity in the workplace ¹⁰. This second feature would possibly become a difficult setting to evaluate. In this certain type of non-physical violence, the behaviors usually become visible due to the growing intensity over time. The negative attacks and feedback that the individual may receive on his or her personal and professional performance are often unpredictable, irrational and unfair. Building in this characteristic of intensity over time, it is also described as an escalating process in the course of which the person confronted ends up in an inferior position and becomes the target of negative social acts.

Table IV.5. Consequences of Bullying

With a global prevalence rate ranging from 11 to 18 %, bullying at work has been linked to a number of detrimental consequences for victims, witnesses, organizations, and the society at large.

Workplace bullying is the result of a complex and dynamic process with contributing causes to be found at various levels, including job design, organization of work, organizational cultures and climate, reward systems, organizational changes, and leadership. In particular, leadership, which is strongly tied to organizational culture, organizational citizen behaviors, and counterproductive work behaviors, has attracted a fair amount of interest from researchers interested in investigating the antecedents of workplace bullying.

Source: L. Francioli et al, "Quality of Leadership and Workplace Bullying: The Mediating Role of Social Community at Work in a Two-Year Follow-Up Study", Journal of Bussines Ethics February 2018, Vol. 147 Issue 4, p. 889–890.

Table IV.6. Experiences of Bullying

Australia: a subcategory of mental stress

In an intend to identify emerging trends in psychosocial health and safety and bullying in Australian workplaces, the second annual national statement issued by Safe Work Australia took used data from accepted workers' compensation claims involving mental stress. As shown in Figure 1, mental stress has clearly reduced while harassment and/or bullying has suffer a light increase. Figure 2 displays the frequency rates of mental stress subcategory clearly presenting the higher exposition of women with respect to men; more than doubling their rates in some cases. Work pressure and work related harassment or workplace bullying get the highest frequencies.¹¹

⁹ M. Coetzee, J. van Dyk, Workplace Bullying and Turnover Intention: Exploring Work Engagement as a Potential Mediator, "Psychological Reports", 2018, Vol. 121(2), p. 376

¹⁰ G. Nami, R.F. Nami, *The bully-free workplace: Stop jerks, weasels, and snakes from killing your organiza*tion, John Wiley & Sons Inc. Hoboken, NJ, 2011

¹¹ https://www.safeworkaustralia.gov.au/system/files/documents/1702/psychosocial-bullying-statement.pdf



Most of the clinical depression cases in Japan categorized as rosai are caused by overworking. Nevertheless, the Kyodo News Agency reported two men working at a company in Yokohama City who became clinically depressed after they had been intentionally assigned no work.12¹²

United Kingdom: the health sector

A study examining the prevalence and impact of bullying behaviours between staff in the National Health Service (NHS) workplace found that 20% of the staff reported having been bullied by other staff to some degree and 43% reported having witnessed bullying in the last 6 months. Male staff and staff with disabilities reported higher levels of bullying. Moreover, the main barriers to reporting the problem were the perception that nothing would change, not wanting to be seen as a trouble-maker, the seniority of the bully and uncertainty over how policies would be implemented and bullying cases managed.¹³

¹² Source: Japan Labor Flash, 2003. Cited in D. Chappell, V. Di Martino, Violence at work. International Labour Organization, 2006

¹³ M. Carter, N. Thompson, P. Crampton, G. Morrow, B. Burford, C. Gray, J. Illing, *Workplace bullying in the UK NHS: a questionnaire and interview study on prevalence, impact and barriers to reporting*, "BMJ open", 3(6), e002628, 2013.

Mobbing

"Mobbing typically involves a group of workers ganging up on a target employee and subjecting that person to psychological harassment. Mobbing includes such Definition and types of Sexual Harassment as making continuous negative remarks about a person or criticizing them constantly; isolating a person by leaving them without social contacts; gossiping or spreading false information about a person; or ridiculing a person constantly"¹⁴. Although this actions might appear of minor impact on the surface, the consequences can be devastating.

It is remarkably important to differ mobbing from bullying. The conceptual distinction between bullying and mobbing is that the first term is primarily referring to situations of individual harassment, whereas mobbing is primarily covering situations of collective harassment.

Even if it is broadly known as mobbing, countries have denominated it with their own words: *harcèlement moral* in France, *acoso or maltrato psicológico* in Spain, *coacção moral* in Portugal or *molestie psicologiche* in Italy¹⁵.

Many experts point at this behaviour as the most important in contemporary organizations. Especially in those countries where there are more SMEs compared to big enterprises. This is due to the hierarchic and the executive nature of both groups. It is different to be directed by a board of directors compared to a single owner. This last profile, will have a notably higher power. Moreover, the employees will more likely have unipersonal positions, where one person has to do many tasks.

Table IV.7. Findings in the Mobbing Arena

Spain

An investigation in 2003, revealed that, around 5% of workers are affected by mobbing in Spain. The same survey repeated in 2012 discovered that the mobbing incidence had increased from 5.84 to 7.06%.¹⁶

A study in the Spanish public administration pointed out that 22 per cent of officials had suffered from this type of violence.¹⁷

Slovenia

The prevalence of mobbing in Slovenia can be compared to data from other countries. About 24% could be classified as regular victims of mobbing.¹⁸

¹⁴ ILO, 2004b, p.a

¹⁵ D. Chappell, V. Di Martino, Violence at work. International Labour Organization, 2006

¹⁶ D. Cglar, G. Tozun, M. Karay, Mobbing Behaviors in Public and Private Banking Sector: A Case Study in Northern Cyprus, "International Journal of Economic Perspectives", 2017, Vol. 11 Issue 2, p. 76

¹⁷ V. Cisneros, *Mobbing in Spanish public administrations report*. Courtesy of Iñaki Piñuel to the authors

¹⁸ D. Mumel, S. Jan, S. Treven, D. Malc, Mobbing in Slovenia: Prevalence, mobbing victim characteristics, and the connection with post-traumatic stress disorder, "Our Economy", February 2015, Vol. 61 Issue 1, p. 3-12

Europe

Mobbing in Europe is very well known, being carefully analyzed by the major research centers and controlled in various meetings. On average, 9% of European workers said they were victims of mobbing in 2015, according to studies conducted by French researchers.¹⁹

Several studies from around the world have confirmed that mobbing is an important problem. Researchers estimate that the prevalence of mobbing ranges anywhere from 1% to 53% among various occupations and countries.²⁰

Discrimination by type

Discrimination is "any distinction, exclusion or preference made on the basis of race, color, sex, religion, political opinion, national extraction or social origin, which has the effect of nullifying or impairing equality of opportunity or treatment in employment or occupation"²¹, and allows additional criteria to be included after consultation by the governments concerned with employers' and workers' organizations. We talk about discrimination at the workplace when it comes to any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoff, training, fringe benefits, and any other term or condition of employment.

This problem which is mostly found at many workplaces, has become more relevant in recent years. Issues affecting sizable groups of the present society have developed into protests and revolutions all around the globe. Discrimination can manifest in many different forms.

Gender Inequality

The most acknowledged type of discrimination nowadays is gender inequality. Historically, inequalities between men and women in labor market outcomes²² have been taken as valid proxies for sex discrimination. It is likely to intersect with other forms of discrimination, such as age or race. Furthermore, it reinforces discrimination in other social spheres such as family, community and school.

There is still a lack of coverage of this type of issues. Nevertheless, laws are adapting in order to take them into account. The US has introduced strict laws regarding different types of discrimination against women. These are listed as follows: Equal Pay/compensation, sex, sexual harassment, and pregnancy²³.

Figure IV.6 evidences how the employment rate for women is always lower compared to men. Figure IV.7 displays the gender wage gap²⁴, which is the difference between median earnings of men and women relative to median earnings of men. This variable also expresses the advantage of men. This group, have higher wages in all countries of the OECD. For Poland, the gender gap in 2016 was 11.1%. It is of great importance the fact that Poland is found below the OECD average for both indicators.

¹⁹ M.L. Romanescu, Mobbing Phenomenon – Factors of Discrimination and Stress, "Annals of the Constantin Brâncuşi University of Târgu Jiu, Economy Series", Issue 1/2017, p. 124

²⁰ D. Mumel, S. Jan, S. Treven, D. Malc, *Mobbing in Slovenia*..., p. 3-12

²¹ ILO Convention No. 111

²² Labour market outcomes used include labour force participation rate, employment and unemployment rates by sex, female share in employment, percentage distribution of women workers by status (unpaid, selfemployed and employee), female shares in legislative and managerial positions and the gender pay gap.

²³ See: https://www.eeoc.gov/laws/types/

²⁴ It is unadjusted. The data refers to full-time employees and to self-employed



Figure IV.6. Employment rate for men and women, % of working age population, Q1 2018

Source: OECD (2018), Employment rate (indicator). Doi: 10.1787/1de68a9b-en (Accessed on 10 June 2018)





Source : OECD (2018), Gender wage gap (indicator). doi: 10.1787/7cee77aa-en (Accessed on 10 June 2018)

Racial and Ethnic Discrimination and Migrant Workers

Racial and ethnic discrimination is also one of the most known type of discrimination. Although experiencing a decline in recent years, it is still a notorious issue. Many countries have had to tackle with civil wars, genocides or other type of conflicts based on race or ethnicity. Also, indigenous and tribal peoples have survive centuries of unequal treatment combined with deep ethnic socio-economic inequalities which have led to less favourable development nowadays. This characteristics make them vulnerable to ethnic stereotyping. Moreover, globalization has come with another type of discrimination due to the intensification of labour migration. Migrant workers, are seen, in many places, as a threat to the native society. Thus, the host population tends to treat them, as well as those of foreign origin, with hostility.

Discrimination Based on Religion or Social Origin

Another remarkable type of discrimination, which has increased in recent years is that based on religion. To disentangle the possible causes that lead to this discrimination is not an easy task. The unbreakable link that religion groups have with specific economic levels is likely to be one, as well as the intensification of migration and the different traditions which cause clashes in cultures. Discrimination based on social origin can also take place at the workplace. This setting can be identified when prejudices and non-institutional practices based on social origin determine the labour opportunities of an employee.

Discrimination by Age

Job attainments and returns to work have increasingly been subject to the age of the person. The causes and consequences on the young and old are broadly differentiated. Moreover, recent surveys point out that the younger suffer more from this problem compared to their older peers. The most known is the payment of lower entry wages under the assumption of low experience, as well as longer probation periods and greater resilience on flexible contracts. It is importantly remarkable as well the fallacy of the substitution between older and younger workers. Proving such type of discrimination, as there is empirical evidence showing that substitution between older and younger workers rarely occurs.



Figure IV.8. Employment rate by age group, % in same group age, Q1 2018

Source: OECD (2018), Employment rate by age group (indicator). doi: 10.1787/084f32c7-en (Accessed on 10 June 2018)

The statistics shown in Figure IV.8 are consistent with the ideas presented. The youngest group 15-24 is the one with the lowest employment rate.²⁵ This could be due to the low experience. The second group with the lowest rate are those between 55 and 64 years old. The employment rate of this group is probably the most volatile when comparing the indicator across countries. Nevertheless, the trend of the order among the three groups remains the same for all countries. As well as the group of age 25-54 having the highest employment rate.

Sexual Orientation Discrimination

Several workplaces are under a rigid and established pattern which does not accept lesbian, gay, bisexual or transgender employees. Given this setting, the sexual orientation or the belief of a sexual orientation would be under judgment, becoming the target of physical and psychological violence and other acts of hate. Homosexuality is illegal in several countries around the world, thus in such states there can be corporal punishment or imprisonment. Nevertheless, international and human rights institutions and mechanisms are increasingly fighting to resolve this issue.

Disabilities and Illnesses

Around 10 percent of the world's population has a mental or physical disability. Most of whom are in a working age. Also, the vast majority of them, live in developing countries. Even if there are different definitions and methodologies to fight this problem worldwide, this group follows a trend of being below the average activity rate. This reflects problems such as the lower educational and skills development attainments as well as the opportunity barriers imposed by society and institutions. Also, some illnesses have been subject to discrimination for years. The most impactful one is the case of HIV/AIDS. In 2016, 36.7 million people globally were living in this condition and around 1.8 million people became newly infected²⁶. Around the 95 per cent of them living in developing countries. The stigma and discrimination surrounding this condition is complex. Either if one has it or is perceived as having it, will suffer from labour discrimination.

Genetic Discrimination

Obtaining the genetic status of individuals has become easier in recent years. In several situations the employers can justify the need of this information for safety reasons, especially in workplaces were the employees are exposed to radiation or chemicals. At the same time, the organization can be dismissing or excluding those who show a predisposition to develop a disease in the future. Thus, it might lead to an unjustified denial of employment.

²⁵ Employed people are defined as those aged 15 and over who report that they have worked in gainful employ ment for at least one hour in the previous week or who had a job but were absent from work during the reference week while having a formal job attachment. This indicator is seasonally adjusted and it is measured as a percentage in same age group.

²⁶ http://www.unaids.org/en/resources/fact-sheet

Discrimination Based on Lifestyle

The lifestyle of the workers is also becoming a determination factor in obtaining or keeping a job. Whether if his or her lifestyle is "healthy" is put under judgement of the organization. Overweight, smoke or hypertension can become clear disadvantages in the labor market.

How to fight against violence at work

International laws

From the creation of the European Union, it has been approved laws of equality between women and men in order to guarantee their fair treatment at work. Initially, these laws only reached the economic sector in the form of equal salaries without covering the social sphere. Over time and the incorporation of women in the workplace, more regulations, directives and recommendations have been included (equal treatment to get a job, protection to pregnant employees, rights on maternity and paternity leave) as principles to fulfil for the whole European community. On the other hand, the efforts to fight against discrimination not only for reasons of sex, but for racial, ethnic origin, religion, belief, disability or age have been achieved in diverse directives approved since 2000 by the Council of Europe.

The following paragraph will describe the main rules at the European Union that regulate the principles of equality, discrimination by race and sex and harassment and sexual harassment at work.

Equality between men and women

The European Union has given special relevance to equal opportunities between women and men and no discrimination by sex in labor market. This concept was link to labour issues and equal opportunities and through the years it has acquired higher dimension and it has been integrated within other policies and European actions. All the directives adopted are mandatory for all the states of the European Union.

- The Treaty of Rome (1957) mentions for the first time the term equality in art. 119 "Each Member State shall during the first stage ensure and subsequently maintain the application of the principle that men and women should receive equal pay for equal work". This first step to equality only embraces salary requirements, without concessions to a broader social perspective.
- With the Treaty of European Union (1992), also known as Treaty of Maastricht, gender equality is a "fundamental value" (art. 2) and an "objective" (art. 3) of the EU.
- The Treaty of Amsterdam (1997) took a further important step by declaring the advancement of equality between women and men to be a fundamental task of the EU (art. 2, 2.3 and 13) and the importance of equality in social policy (art. 136, 137 and 141). Member States are required to eliminate inequality, promote equality between women and men and stand again all forms of discrimination on the bases of gender or other attributes.
- In 2007 the Treaty of Lisbon was approved. Equality understood as "equality between women and men" is referred to as a value of the union. Discrimination is mentioned in art. 3.3 saying: "The Union shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men".

- The charter of Fundamental Rights of the EU and the European Convention for the Protection of Human Rights²⁷ once again reinforces the prohibition of discrimination and the obligation to ensure equality between women and men in all areas. Specifically, in art. 20 where "Everyone is equal before the law" and also in art. 21 "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited". Moreover, art. 23 mentions: "Equality between women and men must be ensured in all areas, including employment, work and pay. The principle of equality shall not prevent the maintenance or adoption of measures providing for specific advantages in favour of the under-represented sex".
- Beyond the European rules, it is important to mention the Convention on the Elimination of All Forms of Discrimination against Women²⁸ (CEDAW), adopted in 1979 by the UN General Assembly, which encourages the States to take all appropriate measures to ensure "the full development and advancement of women enjoyment of human rights and fundamental freedoms on a basis of equality with men in any particular field" (art. 3).

Harassment and sexual harassment

The regulations about harassment and sexual harassment have been incorporated in the following directives of the Council of the European Union and were approved based on art. 19 of the Treaty of Rome:

- The Directive 2000/43/EC²⁹ concerns the application of the principle of equal treatment of people irrespective of their racial or ethnic origin and defines harassment as "an unwanted conduct related to racial or ethnic origin takes place with the purpose or effect of violating the dignity of a person and of creating an intimidating, hostile, degrading, humiliating or offensive environment".
- In the Directive 2002/73/CE³⁰, the regulation acquires an enlarged definition and the term sexual harassment is defined as: "where any form of unwanted verbal, nonverbal or physical conduct of a sexual nature occurs, with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment' and adds: "Harassment and sexual harassment within the meaning of this Directive shall be deemed to be discrimination on the grounds of sex and therefore prohibited".
- Lastly, Directive 2006/54/CE says: "Harassment and sexual harassment are contrary to the principle of equal treatment between men and women and constitute discrimination on grounds of sex for the purposes of this Directive. These forms of discrimination occur not only in the workplace, but also in the context of access to employment, vocational training and promotion. They should therefore be prohibited and should be subject to effective, proportionate and dissuasive penalties" (paragraph 6). This directive requires the implementation of the prohibition of direct and indirect sex dis-

²⁷ https://rm.coe.int/16806f53e6

²⁸ http://www.un.org/womenwatch/daw/cedaw/cedaw.htm

²⁹ https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML

³⁰ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0073

crimination, harassment and sexual harassment in pay, (access to) employment and in occupational social security schemes.

No discrimination by sex orientation or race

- The Human Rights Act 1998 Prohibition of discrimination³¹: The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status (art. 14). Thus, this article is based on the core principle that all of us, no matter who we are, enjoy the same human rights and should have equal access to them. In addition, the whole of protocol 12 is dedicated to the principle of non-discrimination.
- Nowadays, EU law protects people against discrimination based on sexual orientation, age, disability, religion and belief in employment as it says in Directive 2000/78/ EC³². This regulation means that European citizens are legally protected across the EU against: being refused a job or fired because of their sexual orientation and/or being harassed by colleagues at work because you are gay.
- Regarding discrimination by race, The Racial Equality Directive 2000/43/EC³³ prohibits discrimination on the ground of racial or ethnic origin in a broad range of fields, including employment, social protection and social advantages, education, and goods and services available to the public, including housing.

It is important to note that the legal protection against discrimination based on the different grounds varies from one EU country to another. All Member States have legal rules going beyond what is already required by European law, but discrimination on some grounds (age, disability and sexual orientations) will be more or less covered depending on the national laws of each country member.

Across borders of the EU, countries worldwide have been progressively applying several agreements and relevant clauses in order to ensure an improvement in this precise context of compliance³⁴.

Soft law

Soft law refers to "rules that are neither strictly binding in nature nor completely lacking legal significance. In the context of international law, soft law refers to guidelines, policy declarations or codes of conduct which set standards of conduct. However, they are not directly enforceable"³⁵.

³¹ https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/12

³² https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0078:en:HTML

³³ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0043

³⁴ See http://www.ilo.org/wcmsp5/groups/public/-ed_dialogue/-actrav/documents/publication/wcms_546645.pdf. (Violence and harassment against women and men in the world of work : trade union perspectives and action / International Labour Office, Bureau for Workers' Activities (ACTRAV). – Geneva: ILO, 2017.)

³⁵ https://definitions.uslegal.com/s/soft-law

It is often anticipated to legislation. And represents a supportive tool to hard law. In this framework, it is easier to develop immediate and flexible responses to violence or discrimination at work. Laws, however, due to its rigid and statutory character would be, in several cases, are less likely to solve conflicts.

- The first ordinances covering violence and menaces at the workplace appeared in 1993. The National Board of Occupational Safety and Health in Sweden issued two comprehensive and innovative ordinances on workplace violence under the authority of its Work Environment Act. They focus not only on the ordinances, but also on practical guidance to implement provisions and recommendations.³⁶ They nowadays prevail as a remarkable advancement and an unprecedented example for countries around the world.
- Observing the need to take action on workplace violence, on 23 December 2004 the European Commission decided to launch the first stage of consultation of the social partners concerning violence at the workplace and its effects on health and safety at work, in the context of the Commission's own agenda in the field of occupational health and safety, set out in the Community Strategy on Health and Safety at Work for 2002–2006³⁷.
- Of all the problems mentioned in the present report, violence against women is the most covered topic by soft law. The UN Committee on the Elimination of Discrimination against Women (CEDAW) has been supporting normative developments on violence against women that did not exist previous to the birth of the Convention on the Elimination of All Forms of Discrimination against Women. This Committee, approaches the relationship of soft and hard law not as binary, but as an intermediary term to allow easier access to hard law³⁸. The statements the CEDAW does in events, or in General Recommendations published, set new guidelines on what is the path to follow. The last one was the General recommendation No. 37 (2018) on the gender-related dimensions of disaster risk reduction in the context of climate change.
- The EU has supported and encouraged an increased protection of women through soft law, including communication and recommendations. This has provide guiding principles, exchange of best practices, and capacity building. A good example of this is the Daphne Program³⁹, born in 1997, to support victims of violence and combat against future violence.

Compliance in companies

Definition and benefits of compliance

In response to increasing international regulations, organisations have developed tools to adapt to legality. Being in accordance with established legislation is known as the concept compliance. Following these rules means that companies set up policies and adequate procedures to guarantee that companies and all their employees follow the rules. Within this frame-

³⁶ Violence at work, ILO CH1

³⁷ http://www.europarl.europa.eu/hearings/20071121/femm/framework_agreement_en.pdf

³⁸ E. Yahyaoui Krivenko, The Role and Impact of Soft Law on the Emergence of the Prohibition of Violence Against Women Within the Context of the CEDAW. In Tracing the Roles of Soft Law in Human Rights, 2016, p. 47-67

³⁹ http://ec.europa.eu/justice/grants/results/daphne-toolkit/en/daphne-toolkit-%E2%80%93-active-resourcedaphne-programme

work, they also have to consider internal policies, commitment to clients, and ethical codes. Thus, the goal of compliance is to "prevent and detect criminal conduct while promoting an organization's ethical standards and values"⁴⁰. Developing a proactive compliance program benefits not only companies themselves but also society together. Some benefits are easily tangible such as reducing fines; while others go beyond monetary implications. Here are some of the most important advantages:

- Helping organisations to reduce operational and administrative costs (reducing the risk of fines and penalties)
- Improving efficiencies and productivity: employees are more motivated to work when they feel that they are well compensated for their efforts and that they are safe and protected
- Reducing risks of misconducts in workplace
- Improving confidence and trust among employees and clients and potential clients
- Building a positive reputation: compliance will ensure that a company can uphold a positive image and build consumer trust. This also helps build consumer loyalty, since customers are more likely to return to a service or product from a company they identify as trustworthy

Creating a culture of compliance has to go beyond the laws dictated by the International and National Law. It must be present in everyday workflow and be part of the roots of the companies. For this reason, companies must work on building all the necessary tools within their corporate structures in order to follow regulations and develop compliance into a real corporate culture that prove effective over a long period of time.

Building effective guidelines

As we have seen in the previous section, the international law, regional regulations and national rules of each country have set up diverse tools to tackle and act against violent situations within organizations.

In this context, it has been recommended to companies to have with formal mechanisms such as codes of conduct, protocols, policies and guidelines to protect their employees from improper behaviours.

Organisations have the responsibility to protect not only their employees but external people linked to them.

Independently of the size and the sector of the organisations, these have to offer guidelines focusing on preventing, detecting and fighting against criminal and improper conducts. The aim of these tools are to identify who is responsible for administering the program, to provide general information on the business behaviour, to tend to take a "best practice" approach and to offer channels for reporting misconduct or violations.

The main objectives of guidelines are:

- To prevent conflict situations, violence and harassment
- To ensure health and psychological assistance in case criminal conduct
- To ensure legal support

⁴⁰ According to the preeminent standard for compliance and ethics programs – the United States Federal Sentencing Guidelines ("the Guidelines") https://www.ussc.gov/guidelines

To punish the aggressor considering violent acts as an administrative infraction and crime

Using a one-size-fits-all or once-a-year approach to managing risk is not enough. On the contrary, each organisation must adapt their response to its reality, experience, size and develop their norms of prevention. However, through different frameworks there are a minimum point that organisation program should include:

Communication: Make the protocol visible from the top: The usual channels of communication used within companies related to compliance are mostly internal. In some organisations, the execution of a compliance program is carried out by Human Resources while others are choosing to create additional structures around the issue such as the Compliance Department with a Chief Compliance Officer in some cases.

Companies will ensure that current protocols and guidelines are made available to employees whilst also providing proper communication to their staff. This first step is essential for employees to know the existence of a protocol and how to use it properly. The definitions of what constitutes abuse, mobbing, or harassment must be clear and well defined in order for employees know and recognise when these kinds of situations could be happening and especially which are the channels for reporting these misconducts. Moreover, the employees need to know what the penalties are for such conduct.

The communication channels should be diverse and adjusted to the audience and at the same time, they should be easily accessible to review.

The responsibility of leaders is crucial at this point (it will be explained in more detail in the next paragraphs). They is an example to follow by their employees and the responsibility of the success of compliance policy belongs to them. For this reason, it is necessary that leaders are provided with effective resources to operate correctly.

Training and monitoring employees: Training employees is also a key point to the success of a good compliance policy in a company in order to prevent any cases of misconduct. This training has to be regular and adjust to the audience and can be taught in different forms such as workshops, webinars, seminars, E-learning programs etc. Depending on the size of the company it can be implemented at a general level or focus more on each department and has to be done by managers or people in responsible positions that provide a comfortable climate to speak about compliance.

The aim of training and monitoring employees is to allow companies to conduct a full evaluation of the implementation of protocols, while at the same time helping to recognise any improper behaviour among employees and supervisors, as well as preventing any damage before a problem occurs. It could be also a moment to open new lines of communication with employees solve concerns and answer questions and complaints. A serious training programme also demonstrates that the company is taking the care of their employees seriously and stands against any bad behaviour in the workplace.

Providing companies with a *Risk Prevention Plan* is an effective tool to prepare them to foresee risk and to define responses in case of misconducts. Using interviews and documentations collected from companies (public administration, employees, data protection) and tracking them quarterly or annually (depending on the needs) in order to streamline the process and report updated information. Nowadays, several computer tools and pieces of software's⁴¹ have been developed to execute this process.

⁴¹ Such as: Integrum QHSE Risk & Compliance Software, Compliance Software, i-Sight

David B. Crawford, Charles G. Chaffin and Scott Scarborough have developed an Institutional Compliance Risk Assessment Matrix, which is very accurate in producing a risk prevention plan⁴².

Taking proper actions: when a misconduct happens in the workplace, companies have to provide all the internal mechanisms to tackle it and activate procedures to stop these practices.

At this point, employees who need to report a case of harassment that occurs in the organisation must have the effective and available channels. Normally, companies are endowed with internal and anonymous and/or confidential channels to assist in the investigation of sexual harassment allegations. However, others prefer external assistance channels from professional experts (seen as more independent and fair investigations).

In both cases, employees who report an incident that occurs in the company, either as a target or as a witness have to be protected against retaliation from coworkers and supervisors or manager. *Anonymous hotline services* provided by a third-party are effective tools where employees can voice grievances. Companies such as Edcor facilitate an unbiased and impartial method of reporting issues in the workplace.

One of the last advanced tools is an app called Blind which allows users to see if there are existing signs of harassment in a list of companies. It also provides a network where users can discuss topics such as the wage gap, promotion and negotiating salaries.

Creating a culture of compliance in companies

To acquire a successful compliance in companies, it is not sufficient to simply fulfil the regulation imposed by governments or international organisations by publishing policies and codes of conducts. Culture compliance must be embedded in the core of the organisation and integrated into management practices to be effective.

Boosting a real work and family balance culture and effective leadership in organizations will help to develop a strong culture of compliance permanent in time.

Work and family balance

Reaching a suitable working environment in organisations, where employees are protected, is not only a matter of implementation and execution protocols, but building from the ground up good practices, real leadership and adequate cultural organisation.

Organisations with enriching environment systematically facilitate work-family-personal integration and high levels of satisfaction and compromise. Conversely, if we talk about unfavourable or polluted environments, there is neither existence compromise from managerial level nor good policies, and problems of interpersonal relations are frequent. Therefore, the environment in these companies systematically hinders work-family reconciliation. The possibility of inappropriate attitudes, abuses and even violations is probably higher in organisations with this environment.

The IFREI study developed by International Center of Work and Family at IESE Business⁴³ School measures the corporate family responsibility and its impact on people, society

⁴² Effective Compliance Systems: A Practical Guide for Educational Institutions: https://www.corporatecompliance. org/Portals/1/PDF/Resources/past_handouts/Higher_Ed/2008/Mon/RiskAssessmentMatrixQuickReference.pdf

⁴³ IFREI website: http://ifrei.iese.edu/en/

and organizations. After a participation of 40,000 persons in more than 20 countries is has been observer than 50% of countries and companies belongs to a enriching and favourable environment while the remaining 50% represents polluted and unfavourable environment.

Inclusive culture in organisations

Policies and guidelines are convenient and necessary in ensuring that organisations operate free from violation, but are not enough if we want to create an equal environment of respect and tolerance. The importance of an ethical culture in companies in accordance with regulations is not only seeking to fulfil the rules but the commitment from all the departments in the company.

Work-family culture is defined as, "the shared assumptions, beliefs and values regarding to the extent to which an organisation supports and values the integration of employees' work and family lives"⁴⁴. Therefore, a positive ethical culture in companies will be committed to equal opportunities, respect, diversity and zero-tolerance to inequality and harassment at work. Moreover, when a company generates trusted environment of safety and respect, employees will be more comfortable to use available channels if a misconduct behavior occurs.

Having an inclusive and responsible culture also means taking care of employees and consequently having a positive impact in other dimensions such as commitment to workers, equality between men and women, high quality of work and low levels of turnover and work-family conflicts.

For many years, Iceland has been a reference in equality between men and women. In 2018 has become the first country in the world to make companies prove they are not paying women less than men for the same work⁴⁵. Following the Equal Pay Standard, companies and government agencies with more than 25 staff must obtain government certification of their equal pay policies. Although full equality between the sexes had yet to be achieved much had been accomplished in recent years and this law is a clear example.

Leadership and servant leadership (FSSB)

To reach an equal and feasible opportunity for employees within organisations it is required and necessary to have reliable leaders encouraged to promote work and family balance and a healthy environment of respect and zero-tolerance to any kind of discrimination at any level (employees, peers, leaders, or business partners). For any effective program of compliance, the role of leaders is to maintain a culture that actively promotes ethical attitudes and demonstrates good behavior to their employees.

Many studies have evidenced (reference) that having a supportive leadership team makes a huge difference not only in personal happiness but also in benefits of the company and society. Therefore, a real culture of compliance requires top managers to be transparent and honest about their own behavior and take proper ethical conducts that can be spread throughout the whole organisation and taught them in compliance.

⁴⁴ K.A. French, M.D. Agars, Work–Family Culture in Low-Income Environments, "Journal of Career Development", February 2018, Vol. 45 Issue 1, p. 50-67 and: C. Thompson, L. Beauvais, K. Lyness, When Work-Family Benefits Are Not Enough: The Influence of Work-Family Culture on Benefit Utilization, Organizational Attachment, and WorkFamily Conflict, "Journal of Vocational Behavior", 1999

⁴⁵ E. Bjarnason, Ch. Hauser, *Iceland Makes Companies Prove They're Not Paying Women Less* 2018. https://www. nytimes.com/2018/01/03/world/europe/iceland-equal-pay.html?_r=0

A real leadership is effectively exhibited through FSSB (family supportive supervisor behavior), defined as behaviours exhibited by supervisors that are supportive of families. FSSB is construct with four subordinate dimensions: emotional support, instrumental support, role modelling behaviours, and creative work-family management⁴⁶.

The consequences of positive supportive leadership are visible in work-family conflicts, job satisfaction, turnover intentions.

Evaluation, education and being inclusive

Besides the application of formal protocols and programs, organisations should periodically assess and collect data on violence and harassment to know their status. Thus, this will enable them to design a good preventing plan that can reduce the risk of improper conducts. These high-quality data sources allow companies to take the necessary steps to design, implement or modify each element of their current culture of compliance. These methods include external benchmarking, anonymous reporting, pulse surveys, reputation analysis, management communications, audit results, group discussions, facility visits and scores, exit interviews, internal interviews and focus groups.

The research done by academia is a highly relevant tool for governments and institutions when deciding which public policies need to be applied. First, it is important for each country or organization to have a picture of the current situation as a starting point for improvement. Working in this direction, the IFREI Studies conducted by IESE Business School, and mentioned in 1.3 of the present report, analyse countries and companies separately. It distributes the employees in four groups based on the perceived environment they are working in. This enables them to see the weaker aspects of their society. Based on the results from rigorous and scientific analysis governments or enterprises are able to start taking decisions. The B-IN Study, is another benchmark bringing a radiography of the situation in the country. It, in turn, highlights the importance of adopting a culture of being inclusive.

Also, the literature on the subject is highly relevant in order to know and disentangle the effects of having bad practices in the workplace, and to discover the advantages that good practices and a good culture will provide them with. In a recent study, Gluschkoff, K., et al. (2017) found that exposure to violence was associated with an increase in disturbed sleep. Building on the context of FSSB, Hammer et al. (2011) and Kossek et al. (2011) found that it improves both family-specific and more general work and well-being outcomes for employees, such as reduction in the number of family conflicts. Aquino, K., Thau, S. (2009), conducted a relevant study consisting in investigate who is likely to become a victim. In order to achieve it, they look at predictors such as personality, demographic, behavioral, structural, and organizational variables. On a more positive path, Gadergaard, C. A., Anderse, L. P. and Hogh, A., (2015) suggest that prevention behaviors are more effective in relation to a moderate frequency of violence. Enlighting that only top management prevention behavior can prevent very frequent incidents. However the incidence they might have, will vary depending on the sector. Also, the results from Chang, C., et al. (2012) found that organizational policies, prompt management responses to assaults, and putting safety as a priority contributed positively to prevention behaviours through reduced strains and increased motivation.

⁴⁶ Hammer and others (2009)

Examples of companies

In the last years, companies have had to adapt to the regulations and developed a series of tools al mechanism to work on compliance. This article has wanted to show some of examples of companies and countries that are following the right path and could be a model for others.

- Deloitte: The consultancy firm has specifically a service called Governance, Risk and Compliance Services. They provide services of advice and expertise in order to help organization to anticipate and adapt to regulatory change, policies and procedures. Among several report in preventing harassment at work place, a good example is: "Creating a safe work environment Best practices to deal with sexual harassment at the workplace. A Deloitte India survey report"⁴⁷.
- Pwc: the account firm PricewaterhouseCoopers also has a department of Compliance and Risk Management Solutions. They help business to harden compliance and ethics rights into their initiatives. They propose methods, surveys, studies, guidelines and recommendations in order to improve the culture of compliance in organizations⁴⁸.
- Seat: a good example of code of conduct is which has adopted SEAT. The Spanish automotive firm has integrated in his policies an specific section mentioning equal of opportunities and treatment⁴⁹.
- Netflix: Netflix has been target in the last year as one of the best place to work in terms of cultural environment according to Forbes50. Blind, the anonymous employee chat app has launched a survey, where Netflix has been ranked as one of the best within tech's biggest companies in terms of job satisfaction and intentions of turnover⁵¹. Moreover, the firm published in 2009 one of the most viral presentation to date "Netflix Culture". Presenting how they operate in terms of hiring, firing and rewarding employees has been used for others firms as a recruiting tool⁵².
- Cookie Box: An example of company working on developing and transformation people in organizations in terms of compliance and ethical values is Cookie Box [1]. This consultancy in Human Resources implemented a campaign to raise awareness of workplace harassment through a series of videos in an important Spanish firm called Abertis with the goal of helping employees identify cases of harassment⁵³.
- Thomson Reuters: offers compliance training courses on Preventing Discrimination and Harassment, workplace diversity and also surveys to implement at companies⁵⁴.

⁵² https://www.slideshare.net/reed2001/culture-1798664/4-Seven_Aspects_of_our_Culture_

⁴⁷ Creating a safe work environment Best practices to deal with sexual harassment at the work place. A Deloitte India survey report (2016) https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-antisexual-harassment-report-noexp.pdf

⁴⁸ Getting ahead of the watchdogs: Real-time compliance management 2018 State of Compliance https://www. pwc.com/us/en/risk-assurance/state-of-compliance-study/assets/pwc-2018-state-of-compliance.pdf

⁴⁹ SEAT Code of Conduct (Spanish version) http://www.seat.es/content/dam/countries/es/corporate/codigo-deconducta/pdf-codigo-de-counducta.pdf

⁵⁰ W. Aruda, 5 Great Companies That Get Corporate Culture Right. 2017. https://www.forbes.com/sites/ williamarruda/2017/08/17/5-great-companies-that-get-corporate-culture-right/#9e48abc15828

⁵¹ J. Bort, *Netflix Employees Are Happier With Their Job Than Facebook or Google Employees* 2017 https://www.inc. com/business-insider/tech-employees-anonymously-rate-companies-work-facebook-google-netflix-twitter.html

⁵³ For more information: http://cookiebox.es/en/work/hablando-de-lo-que-nadie-habla-el-acoso-laboral/

⁵⁴ The advantages of a global compliance training solution: https://risk.thomsonreuters.com/en/products/onlinecompliance-training.html

We can find as many code of conducts as organizations analysed. The following link shows the best outstanding examples of code of conducts from big firms: https://i-sight.com/resources/18-of-the-best-code-of-conduct-examples/.

UTILIZATION OF NEW TECHNOLOGIES

Methods related to HR management are based on behavioural analysis and detection of hidden relations. The methods employing voice and visual analysis provide assistance during the recruitment process by means of emotional state identification (mood detection), detection of deceptive intentions or abnormal behaviour (also suitable for honesty maintenance, i.e. management of the already employed people, which all belong to a broader category of internal fraud prevention solutions), and identification of financial interrelations.

IT Solutions for HR

LVA-i

Description

The offered platform is an innovation based on Nemesysco's Layered Voice Analysis (LVATM), a technology dedicated to identification of deceptive intentions by extraction of certain vocal parameters correlated with key human emotions. This solution provides realtime insight in subject's mental state and, using signal processing algorithms, enables to detect anomalies and classify them according to a certain emotional state, such as stress, excitement or confusion. It is worth noting, that the LVA is a proprietary technology of Neme-sysco and can be applied over telephone lines and standard microphones. Moreover, the core technology can be adapted to various applications, including pre-employment procedures, personality tests and intermittent "honesty maintenance".

Manufacturer's description

Name: Nemesysco Ltd

Description: Nemesysco, founded in 2000, is a provider of solutions based on voice analysis technology "Layered Voice Analysis", patented by Amir Liberman, the company's CEO, which allows personality and risk assessment. The headquarters are located in Israel, while the offered services are globally distributed by a network of partners in over 50 business locations.

Available product options

Product is available as software for analyst's computer workstation using Voice over IP interface or connected to phone via a special connector provided by Nemesysco.

Expected benefits

- Identification of internal frauds
- Stopping theft and embezzlement
- Preventing leakage of information
- Enhancement of hiring practices

Recommendations / users' opinions

User description: Duke University is a private institution with a long academic tradition, founded in 1838. The main campus is located in Durham, North Carolina, U.S. Duke university offers a variety of highly ranked graduate programs, including Fuqua School of Business, School of Medicine and Pratt School of Engineering.

Benefits/opinion: "We find that higher levels of positive (negative) affect, as operationalized via higher levels of excitement (cognitive dissonance) determined by proprietary LVA software, convey good (bad) news about future firm performance..." [5] – William J. Mayew, Mohan Venkatachalam.

User description: University of Tsukuba is a Japanese public academic institution. The university was established in October 1973, as a result of relocation and transformation of the Tokyo University of Education. Currently, University of Tsukuba is placed on the 250th position in QS World University Ranking.

Benefits/opinion: "Psycholosoft, a research group affiliated with the Department of Psychology at Japan's Tsukuba University, determined that Nemesysco's Layered Voice Analysis (LVA) technology is a reliable and valid tool for detecting mental stress through speech" [5] – Seishin Igaku.

User description: Mamata medical college is a private medical college, founded in 1998. The main building and teaching hospital are located in city of Khammam, Telegana, India.

Benefits/opinion: "A significant correlation was seen between the emotional factors and certain personality traits... Thus the emotions displayed through voice can be used as a tool to determine personality" [5] – Brinda Manchireddi, Josef Kamalesh, Sumaiyah Sadaf, P. Aravind Reddy.

- www.nemesysco.com/speech-analysis-technology
- www.nemesysco.com/pre-employment-hr-recruitment-lvai
- www.nemesysco.com/about-us
- www.crunchbase.com/organization/nemesysco
- · Brochures disclosed by Nemesysco staff
- library.duke.edu/rubenstein/uarchives/history/articles/narrative-history
- www.usnews.com/best-colleges/duke-university-2920#close-modal
- · www.topuniversities.com/universities/university-tsukuba
- www.mamatamedicalcollege.com
- www.targetadmission.com/colleges/12591-mamata-medical-college-khammam

THE DEEPEYES SOLUTION

Description

The DeepEyes solution is an innovative product, artificial intelligence (AI) platform, designed to detect the emotional state of a subject through analysis of micro expressions. Real time analysis is provided by combining statistical and mathematical modelling together with machine and deep learning technologies. Relying on the data acquired by a simple HD camera, the software conduct analysis of video material and performs face recognition, as well as, emotions identification. By means of AI-assisted video processing, this solution provides insight in emotional state, which is suitable for identifying learning conditions and assistance during recruitment process.

Manufacturer's description

Name: DeepEyes

Description: DeepEyes is an IT solution provider for risk assessment and business analytics. The main product offered by the company is software designed to perform computer vision analysis. The company was founded in 2015 and, currently, actively operates in Germany, the Netherlands and the United Kingdom.

Available product options

Since the DeepEyes algorithm is relatively undemanding, the software can be installed on a conventional computer workstation or a mobile device equipped with an HD camera. Moreover, the software does not require an Internet connection.

Expected benefits

- · Enhancement and accelerating of the training process
- Assistance in identification of candidate's suitability for a position
- Improvement in performance management
- Detection of potential internal frauds

- www.deepeyes.co/industries/
- · www.deepeyes.co/industries/human-resources/
- www.deepeyes.co/deepeyes_team/
- www.crunchbase.com/organization/deep-eyes

BEATING INTERNAL FRAUD

Description

The offered solution comprises a risk-management platform for detecting and preventing internal frauds. The working principle of the software is based on analysis of complex employee profile built with the help of behavioural analytics and machine learning. In particular, the software provides real-time monitoring of unusual behaviour of employees, including privileged users, such as IT and database administrators. It is especially suitable for internal fraud prevention in banks.

Manufacturer's description

Name: Netguardians

Description: Netguardians is a Swiss company founded in 2007 and offering innovative solutions for fraud prevention and risk assessment. The company was created with the help of Swiss innovation incubator Y-Parc, in Yverdon-les-Bains, and industry investors, including Swisscom, a leading telecommunications provider in Switzerland. Currently, the head-quarters are still located in Switzerland, however the company also has branches in Nairobi, Warsaw and Singapore.

Expected benefits

- Internal fraud prevention and detection in real time
- 80% reduction in the number of false positive alerts
- Improving operational efficiency by 93%, reduction of the time needed for manual decision
- Fraud losses reduction amounting to 60%
- Rapid implementation

Recommendations / users' opinions

User description: Acleda Bank Cambodia, established in 1993, is currently one of the biggest retail banks in the Kingdom of Cambodia. Since 2003, it has been operating as a full commercial bank with a license granted by the National Bank of Cambodia. Now, this bank has 261 branches and provides its services in all provinces of the country.

Benefits/opinion: "We can detect fraud more quickly and stop it before it happens. It means we've got a lower risk profile, compliance is easier and fraud is down" [1] – Tauch Kampoul, Vice President & Head of Security Operations, Acleda Bank.

- www.netguardians.ch/beating-internal-fraud/
- www.netguardians.ch/about#the-company
- Netguardians, Beating internal fraud solution brief
- www.acledabank.com.kh/kh/eng/bp_fact_figure
- www.acledabank.com.kh/kh/eng/ff_history

INACT INTERNAL FRAUD MANAGEMENT

Description

This comprehensive cross-sectional solution is designed to detect and prevent operational errors, compliance breaches, as well as all types of misconduct attempted by employees, customers, policyholders, brokers, agencies, experts, and service stations. It identifies unusual behaviour and hidden relationships through predictive anomaly detection and financial relationship network analysis. It allows to monitor all financial and nonfinancial transactions, and thus prevent attacks by covering multiple channels simultaneously, including internet banking, mobile banking, branches, ATM, POS, and vPOS.

The conceptual framework of the solution is primarily based on detecting attack scenarios, which are individually established for each client. As such, it helps to detect anomalies which are either a result of fraudulent or erroneous activity. The user can create additional scenarios using an intuitive GUI-based wizard.

Manufacturer's description

Name: Asseco Poland S.A.

Description: Asseco is a Polish software vendor established in 1991, with headquarters in Rzeszów, delivering software solutions and services to the banking and financial services industry, as well as the public sector. Being one of the largest software producers in Europe, present in over 50 countries all over the world, employing more than 24,000 people, the company has been listed on the Warsaw Stock Exchange (GPW Main Market) since 2004.

Available product options

- · This is a highly customized solution implemented in close cooperation with the client
- Can include tailored modules fitted to the client's current IT framework and particular needs

Expected benefits

• Prevents external as well as internal fraud attempts

Recommendations / users' opinions

User description: GarantiBank NV – a mid-sized European bank established in Amsterdam in the Netherlands in 1990. It provides services to retail, corporate and institutional clients. A subsidiary of Turkiye Garanti Bankasi A.S. Managed total assets of around EUR 4.3B in 2017 [4].

- www.pl.asseco.com/o-asseco/profil/
- https://inact.asseco.com/inact-internal-fraud-management/
- https://inact.asseco.com/wp-content/uploads/2017/10/Garanti-Bankas%C4%B1-Hollanda-InACT-ENG.pdf

- https://www.garantibank.eu/uploads/100/GBI%20-%20Annual%20Report%202017.pdf
- Source: Own elaboration

CONCLUSIONS

- The protection of the rights of workers in organizations has been present since the firsts Treaties in the European Union and progressively been enlarged in the last years with the implementations of national rules, agreements and norms in each State Member. Consequently, organizations have had to adapt to external regulations and implement internal compliance programs to adjust their actions to the norm.
- Organizations have expressed an increasing interest to apply compliance programs not only to prevent legal, economic and reputation problems, but to be compromise to the protection and equality of workers.
- Although it seems that compliance has arrived in major companies to a greater or lesser extent, a lot remains to be done to create a real compliance environment. For some countries, culture of compliance is more developed compared to others. For instance, organizations in Germany and in the US have been working more deeply in their cultural programs developing their own compliance departments and having effective external support. On the other hand, in some southern European countries such as Spain or Portugal compliance is still a formal norm that is not yet enough consolidated to protected all the workers.
- Compliance has to be integrated at all hierarchical levels in an organization and be executed from specific departments. Internal protocols, guidelines and codes of conduct have to be accessible to all employees and be implemented more than in everyday practice. Moreover, an appropriate training will be a necessary tool to understand what compliance is and how skipping it could affect them.
- Besides internal policies, the role of leaders in organizations is a basic pillar to effectively make the employees follow the rules and behave in an ethical way. Leaders should be proactive in cultural compliance and transmit ethical values to their employees so that they can see him or her as an example. Moreover, if unlawful conduct is suspected, specific departments but also the leaders should take the initiative to take proper actions in the matter.
- At the same level as external regulations, internal policies and positive leadership, culture in organizations are part of the equation to achieve a true culture of compliance. If organizations create a health and trust environment and take care of their employees, these will be less in favour of acting irresponsibly.

TECHNOLOGY FOR ENTERPRISE SECURITY AND CRIME PREVENTION

INTRODUCTION

The technologies in which large enterprises now find themselves completely immersed are deep, complex, and changing rapidly. Making a decision in such a context is very difficult. Such decisions aren't merely risky – leaders of large enterprises manage risk all the time – rather these decisions are subject to high levels of uncertainty. Leaders and managers simply don't have enough information, or the right information, to make wise choices.

This report is a step towards improving the level of information available to leaders and managers concerning the key technologies that are shaping the future. The first section covers the conceptual background to these technologies. It includes essays on such critical issues as Big Data, Artificial Intelligence, Cyber Security, and the Internet of things. These concepts represent technology developments that are completely altering the landscape. Like it or not, decision-makers must be comfortable in this landscape.

This landscape is full of exciting developments that can improve the way large enterprises operate and increase the satisfaction of customers and citizens. But it is also a landscape that is full of dangers. Every new opportunity in these technical domains brings with it the possibility of some new threat. These dangers can be the work of deliberate, hostile actors who also have access to exciting new technologies. The kinds of criminals are by now well known.

But some of these dangers are simply examples of how technology can turn a small mistake in to a large one. Big data can be a mine of information to make a business competitive. It is also a terrifying liability. An enterprise that accidently exposes the personal details of customers or citizens to the whole world could face an existential crisis.

This review of the perils and promise of the current technological landscape is followed by a section that reviews a wide range of solutions. These are specific technologies that secure data, make transactions easy and safe, or parse vast quantities of information in order to detect technological change. The goal is not to offer all the products, ready to go, that an enterprise might need. Rather it is to expose the user to the details of these kinds of applications. Some of the technical discussions may seem too abstruse, but there is value to touring the technical waterfront, as it is right now.

CONCEPTUAL BACKGROUND

Big Data, Artificial Intelligence (AI) and Machine Learning (ML)¹

"Big data" are sets of data and data management challenges whose size or type is beyond the ability of traditional relational databases to capture, manage, and process.

Big data comes from sensors, devices, video/audio, networks, log files, transactional applications, web, and social media - much of it generated in real time and in a very large scale.

Big data techniques allow users, researchers, and businesses to use and analyse data sources that were previously inaccessible or unusable, independent or together with their existing enterprise data to gain new insights resulting in better and faster decisions. Big data uses techniques such as text analytics, machine learning, predictive analytics, data mining, statistics, and natural language processing.

Big data includes the concept of "three V's":

- *Volume*: Ranges from terabytes to petabytes of data. For instance, a single jet engine can generate 10TB of data in 30 minutes. With more than 25,000 airline flights per day, the daily volume of just this single data source runs into the Petabytes.
- *Variety:* Includes data from a wide range of sources and formats (e.g. web logs, social media interactions, ecommerce and online transactions, financial transactions, etc.). Traditional data formats tend to be relatively well defined by a data schema and change slowly. In contrast, non-traditional data formats exhibit a dizzying rate of change. As new services are added, new sensors deployed, or new marketing campaigns executed.
- *Velocity:* Increasingly, businesses have stringent requirements from the time data is generated, to the time actionable insights are delivered to the users. Therefore, data needs to be collected, stored, processed, and analyzed within relatively short windows ranging from daily to real-time.

Tools for big data address the entire data management cycle, making it technically and economically feasible to collect and store large datasets, and analyze them in order to uncover new and valuable insights:

- *Capture/Collect:* Collecting the raw data transactions, logs, mobile devices and more allowing developers to ingest a wide variety of data from structured to unstructured at any speed from real-time to batch.
- *Store:* Secure, scalable, and durable repository to store data prior or even after processing tasks.
- *Process & Analyze:* Transforming data from its raw state into a consumable format usually by means of sorting, aggregating, joining and even performing more advanced functions and algorithms.
- *Consume & Visualize:* High-value, actionable insights from data assets. Ideally, data is made available to stakeholders through self-service business information and agile data visualization tools that allow for fast and easy exploration of datasets. Depending

¹ What follows is informed by Varian, Hal, 2017 "Artificial Intelligence, Economics, and Industrial Organization" http://www.nber.org/chapters/c14017.pdf, Marcus, Gary, 2017 "Deep Learning: A Critical Appraisal" https:// arxiv.org/pdf/1801.00631.pdf and McKinsey Global Institute, 2017 "Artificial Intelligence: The Next Digital Frontier"

on the type of analytics, end-users may also consume the resulting data in the form of statistical "predictions" – in the case of predictive analytics – or recommended actions – in the case of prescriptive analytics.

Common Uses of Big Data

Understanding and Targeting Customers: This is one of the biggest areas of big data use today to better understand customers and their behaviours and preferences, and in many cases, create predictive models. Big data is at the heart of modern Customer Relationship Management (CRM) systems.

Understanding and Optimizing Business Processes: Big data is also increasingly used to optimize business processes. Retailers are able to optimize their stock based on predictions generated from social media data, web search trends and weather forecasts. One particular business process that is seeing a lot of big data analytics is supply chain or delivery route optimization.

Personal Quantification and Performance Optimization: Data generated from wearable devices such as smart watches or smart bracelets. It gives individuals rich insights, while the real value is in analysing the collective data.

Improving Healthcare and Public Health: The computing power of big data analytics enables us to decode entire DNA strings in minutes and will allow us to find new cures and better understand and predict disease patterns.

Improving Sports Performance: Most elite sports have now embraced big data analytics. The NFL has developed its own platform of applications to assist all 32 teams in making the best decisions based on everything from the condition of the grass on the field, to the weather, to statistics about an individual player's performance while in university.

Improving Science and Research: Science and research is currently being transformed by the new possibilities big data brings.

Optimizing Machine and Device Performance: Big data analytics help machines and devices become smarter and more autonomous.

Improving Security and Law Enforcement: Big data is applied heavily in improving security and enabling law enforcement. Big data techniques are used to detect and prevent cyberattacks. Credit card companies use big data use it to detect fraudulent transactions.

Smart Cities: Big data is used to improve many aspects of our cities. For example, it allows cities to optimize traffic flows based on real time traffic information as well as social media and weather data. A number of cities are currently piloting big data analytics where the transport infrastructure and utility processes are all joined up. Where a bus would wait for a delayed train and where traffic signals predict traffic volumes and operate to minimize jams.

Financial Trading: Today, the majority of equity trading now takes place via data algorithms that increasingly take into account signals from social media networks and news websites to make, buy and sell decisions in split seconds.

Small versus Big

Small data is big data derived from local sources. This connects people with timely, meaningful insights and is organized and packaged to be accessible, understandable, and actionable for everyday tasks. There are several good reasons for working with "local" or small data. Big Data is hard: Doing it at scale and waiting for trickle down benefits can take time.

Small data is all around us: Small data that is ready to be collected to inform and make decisions. Small data is at the center of Social CRM: used to create a complete picture of customers, their segments, influencers and even competitors, small data is the key to building these rich profiles that will be the center of the new CRM solutions.

Platform and Tool vendors are starting to pay attention: The promise of operationalizing Big Data and "turning insight into action" is a major tone from many of the big names in tech including SAP, Oracle and EMC. It's all about the end-user. In practice, its small data that is about the end-user, what they need, and how they can take action. Focus on the user first, and a lot of technology decisions become clearer. You shouldn't need to be a data scientist to understand or apply data analysis for everyday tasks.

Analytics are the mechanisms for turning data, big and small, into useful information that can be used to guide action. Analytics can be divided into three types:

- Descriptive analytics help users answer the question: "What happened and why?" Examples include traditional query and reporting environments with scorecards and dashboards.
- Predictive analytics help users estimate the probability of a given event in the feature. Examples include early alert systems, fraud detection, preventive maintenance applications, and forecasting.
- Prescriptive analytics provide specific (prescriptive) recommendations to the user. They address the question – What should I do if "x" happens?

Increasingly, Artificial Intelligence (AI) and Machine Learning (ML) are at the heart of the analytics employed in understanding and using data.

Artificial Intelligence and Machine Learning

Imagine a set of digital images and a set of labels that describe what is depicted. It is possible use these data to train a computer to learn how to predict labels for a different set of digital images (or sounds). This has been achieved by training neural networks with multiple layers, made possible because of increases in computational power. This has made deep learning truly practical for the first time. This approach has been remarkably successful with image recognition, voice recognition, language translation and other challenging machine learning activities. Today, computers can outperform humans in many of these tasks.

This approach, called deep learning, requires 1) putting labels on data for training, 2) developing algorithms for the neural networks, and 3) building specialized hardware to run the algorithms. It is important to have experts who can manage the data, re-work the algorithms, and oversee the entire process. These skills are the main bottleneck at the moment in the widespread application of AI.

Neural networks typically consist of a set of input units that stand for things like pixels or words, multiple hidden layers (the more such layers, the deeper the network) containing hidden units or nodes, and a set of output units, with connections running between input units, nodes, and output units. This kind of network might be trained on a large set of images as inputs and on labels as the outputs that identify the categories to which those inputs belong. For example, this image is a puppy, that one is a fish, and so on.

An algorithm allows a process to occur that adjusts the connections between units, so that any given input tends to produce the appropriate corresponding output. These connections are increasingly described as neural networks. The relation between inputs and outputs in a neural network is a kind of mapping. Neural networks, particularly those with many layers are very good at learning input-output mappings.

Such systems are described as neural networks because the input nodes, hidden nodes, and output nodes can be thought of as loosely analogous to biological neurons, (although this is a highly simplified analogy), and the connections between nodes can be thought of as reflecting connections between neurons.

Examples of Machine Learning in the popular press emphasize applications such as winning at chess. However, there are many applications that use machine learning to solve realworld business problems. All you need is some data, a problem, and some resources to buy the services of data scientists.

Applying Machine Learning

Suppose you want to develop a machine learning system in your organization. What are the necessary pieces of the puzzle? First, you need a data system that collects and organizes the data you are interested in understanding. For example, an insurer would need a system that can collect data from individual policy holders, and then upload it to a computer that can then organize the data, and combine it with other data, such as financial data, and information about the customer. Once the data has been organized, it can be collected together to in a data warehouse. The data warehouse allows access to a system that can manipulate and analyze the data. In the past companies have run their own data warehouses which was complicated and expensive.

It is now more common to store and analyse the data in a cloud computing facility. The cloud provider takes care of managing the hardware and software necessary to host the database. An organization can purchase virtually any amount of cloud-based services, so even small companies can participate. Renting time on a cloud-based system is much more cost effective than owning a data center since resources can be purchased as needed. Many startups today use a cloud provider for their hardware, software, and networking needs.

Cloud providers also offer various machine learning services such as voice recognition, image recognition, translation, and so on. These systems are already trained and can be put to use immediately by the customer. It is no longer necessary for each company to develop its own capabilities for these tasks. Competition among providers is intense. For example, highly detailed recognition capabilities are offered at a penny or less per image.



Figure V.1. Relationship between data, information, and knowledge

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

If the hardware, software, and expertise are available, all that is needed is data with labels. There are a variety of ways to acquire such data; for example, data drawn from operations, data scraped from the web, data purchased from private or public providers, and data obtained by sharing and exchanging with others.

Information science uses the concept of a "data pyramid" to show the relationship between data, information, and knowledge.

A system collects the raw data, it is then organized and analyzed. Next synthesis converts analysis into knowledge, and wisdom turns knowledge into action in the world. In contrast to markets for knowledge – books, theorems – markets for data are not as fully developed.

Challenges

In fact, deep learning, or Machine Learning (ML), has a variety of limitations. Deep learning works less well when there are limited amounts of training data available, or when the wider world studied by the system is very different from the limited world in which it was trained. Furthermore, machines don't get "smarter" as the size of the data sets with which they work grow. More data is subject to diminishing marginal returns. Finally, some problems cannot be thought of as classification problems, which is the activity at which Machine Learning excels.

Data ownership and data access are very sensitive questions. The EU is addressing them through the General Data Protection Regulation (GDPR). (EU) 2016/679 is a regulation under EU law on data protection and privacy for all individuals within the European Union.² It also addresses the export of personal data outside the EU. The key question is less who is holding the data, and more a question of who has access. Data, including personal data, can be shared widely, without the knowledge of the individuals whose data are included. Regulating who has access, and how it can be shared, is very important, but it will also will place limits on opportunities for new machine learning initiatives.

Large enterprises, with existing capabilities in the digital world, are best situated to exploit AI and ML. But it requires finding the right talent and developing use cases that bring value to the enterprise. AI can help enterprises secure systems and facilities, understand opportunities and threats, target customers more effectively, and increase customer satisfaction. What is evident is that early adopters will obtain benefits from these advantages, develop a wide range of experience with the technology, and attract the necessary talent. This will place them far beyond competitors and adversaries.

The Future of the Internet of Things

The Internet of "Things" (IoT) has the potential to encompass and instrument an enormous range of connected devices – including home appliances and utilities, wearables, homes and corporate buildings, industrial processes, medical devices, law-enforcement devices, military equipment, and other connected applications that today might be barely imaginable. In the present context, "Things" are simply those computerized and networked devices that become part of the IoT. Some of those "Things" will be directly accessible over the Internet, whereas others would be supposedly hidden in local networks behind firewalls and addresstranslating routers.

² https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

There are already many risks recognizably associated with the IoT. Some risks are old and well known but exacerbated by the unprecedented scale of the IoT; estimates for the next few years suggest tens of billions of "Things". Other risks may be new, stemming from the nature of how these "Things" are designed, what they are used for, how they are deployed and managed (or not managed), and how market forces will influence the development. This section outlines some of those risks and what might need to happen if the IoT is to deliver the benefits envisioned for it – with a reasonable level of trustworthiness. This discussion is relevant to everyone involved as a user.

Security and privacy are both extremely important in the IoT, because the potential consequences of successful attacks could impact human lives and safety, and cause death and destruction – directly or indirectly. Privacy violations that let criminals exploit information about potential victims can also constitute threats to safety.

Things Turning Evil

A recent distributed denial-of-service (DDoS) attack has demonstrated the ubiquitous vulnerabilities in the current still-primitive Internet of "Things". Many devices including closed-circuit TV cameras, cable set top boxes, and digital video recorders (DVRs) were compromised and used as unwitting botnet zombies. This significant event used malware (Mirai) that searches for vulnerable victims, and whose source code had been freely published.

By targeting the DNS services provided by Dyn, this attack seriously interfered with user access to major services such as Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix. In one fell swoop, it exposed the tip of just one of many hazardous icebergs. While earlier DDoS attacks using Mirai had exploited hundreds of thousands of devices, this attack appeared to involve tens of millions of compromised devices.

The attack illustrates some of the risks associated with having very large numbers of inadequately protected "Things" connected to the Internet – particularly "Things" that are simple enough to be vulnerable to compromise, but sufficiently capable to be part of a distributed attack that floods the victims' sites with seemingly legitimate requests. Note that the owners or users of compromised devices are often not aware their devices are being used to attack other systems.

Vulnerabilities

Evidently, many of these devices that unwittingly contributed to that DDoS attack were not actually behind any sort of firewall, or else had weak default firewall configurations that were easily exploited. Furthermore, some of the "Things" infected by Mirai were themselves small-office or home-office routers. While Mirai specifically exploited hardcoded passwords for Telnet/SSH services that users could not disable, it is generally foolish to put all the blame on any one weak link, when almost everything is a potential weak link.

Today, almost every computer related system is likely to be already compromised, or else easily misused. We have weakness in depth and breadth, not strength in depth. Therefore, many problems will need to be overcome to make the IoT viable. We consider some of those problems, and some possible remediation. Ultimately, we need a total-system perspective that addresses the potential vulnerabilities in the devices, the alleged firewall security, the network connections, the cloud services (some not even known to the users), and the Internet itself, as well as all its users and would-be malicious actors. The IoT is not an entity per se – it encompasses all of these entities and inevitably depends on them.

We suggest recent DDoS botnet episodes are merely a harbinger of events to come. IoT risks in the future will be pervasive, including potential compromises of requirements relating to trustworthiness. Such requirements must address network-wide issues such as human safety, security, reliability, robustness, resilience, functional interoperability, seamless ease of installation and use, rapid automated remediation of serious flaws, personal as well as institutional privacy, human well-being, and much more.

The Internet of Things' Risks

Denial-of-service attacks are damaging, but the ability to subvert "Things" remotely for arbitrary manipulation must be considered particularly threatening. Here are just a few examples of application areas where the use of IoT devices brings inherent risks:

- Hospitals and healthcare establishments tend to use devices that are already remotely controlled or accessible "Things": patient monitors, body scanners, pacemakers, defibrillators, infusion pumps, main and auxiliary power, lighting, air conditioning, and much more.
- Critical infrastructure sectors such as electric power, oil, natural gas, manufacturing, and transportation use IoT devices as sensors and actuators for automation and remote monitoring and control. The controllers themselves may be Internet accessible.
- Self-driving and automation-assisted interconnected automobiles must clearly be considered as "Things", especially in automated highways of the future. Recent demonstrations of the ability to remotely take over critical vehicle controls illustrate just a few of the risks.

Unlike general-purpose computers, IoT devices may be more closely associated with the physical world. While there have so far been relatively few cases where physical destruction has been intentionally caused through computer compromise, this is likely to be a risk of serious concern for the IoT. From the known cases of programs in the 1960s that could exercise disk arms to cause the drives to self-destruct, to the 2007–2010 Stuxnet attack that appeared to be designed to damage nuclear enrichment centrifuges (and reportedly succeeded), cyber-physical attacks have exploited vulnerabilities that are features rather than flaws.

In addition to the "Things" that control switches, valves, and motors, many "Things" have batteries – which suggests the potential ability to remotely cause certain devices to overheat enough to cause a fire or explosion. If vehicles or medical devices are remotely taken over by malicious attackers, people could be injured or killed by someone clicking from anywhere on the Internet. Manipulation of sensors or insertion of misinformation could indirectly cause other health hazards by inducing chemical spills, disrupting energy systems, or misrouting vehicles. Thus, human safety must be a fundamental issue for many types of "Things".

Another critical difference between IoT devices and general-purpose computers involves management. For a desktop computer, laptop, tablet, or smartphone, there are rich interactions between users and devices. Some notion of management also must exist: for corporate devices there are system administrators in important designated roles, while for personal devices the user is typically also the administrator. However, for IoT devices, there may be very little room for user interaction, and the concept of 'management' is unclear.
While operating systems and applications for general-purpose computers in desktop, laptop, tablet, or smartphone form factor tend to be easy to keep updated, many IoT devices are difficult or impossible for users to update. Some devices will remain in use for their entire lifetimes, precisely as delivered – unless they are recalled, discarded, or just forgotten. In some of those cases, security updates will be essentially impossible or extremely difficult. In other cases, devices may be directly accessible remotely over the Internet; any update mechanisms must be secured so that attackers cannot subvert them and insert their own updates or attacks.

For "Things" that necessarily have interactions with human users, their small size typically will not allow for touchscreens or keyboards. Thus, they must either rely on another device such as a tablet or smartphone for interaction, or else use other emerging modes of interaction such as voice inputs. For voice interfaces, there are problems with linguistic ambiguities, and obvious privacy risks associated with ubiquitous devices that continuously record and process voice conversations, as well as interesting opportunities for replay or synthesized voice-command attacks from one device to another device. As already evident in advertising applications, audio interfaces could also be used for covert ultrasound communication, inaudible to humans.

Whereas botnet attacks may typically be stopped by blocking the command and control servers that orchestrate the attacks, the individual IoT devices are still compromised, and could be pulled into a new botnet at any time. We are left with many questions. For example, who is responsible for fixing these devices? What incentive would the owner of a connected camera have for going through the trouble of updating its firmware if it seems to work just fine as it is? Who is liable when major disruptions occur? Is it the manufacturer, the vendor, the person or organization who deployed the device, the cloud or back-end communications provider, or the unwitting user of the device? Each of these alternatives entails its own set of risks.

Until recently, consideration of most of these risks has been dominated by the competitive rush to market, with very few concerns for trustworthiness. This reality tends to cause security and privacy to be sadly neglected. Clearly, that must change, suggesting the advent of some serious far-sighted systemic considerations – especially where the risks might be greatest.

Confronting the Risks

We next attempt to outline some steps that might be desirable. As has been noted in the past, we have a serious need for considering risks in the context of total systems. The Internet of "Things" requires much deeper concern for total-system trustworthiness, in which the security of "Things" is only one aspect – especially because at the moment there is essentially no real security in computer systems and networks. This reality is clearly making the problems of assuring trustworthiness much more difficult.

We enumerate here just a few of the steps that might be helpful for developers, administrators, and users. However, we explicitly caution that this summary is only an essential beginning, and inherently incomplete. It may not be surprising that what is needed is more or less consistent with the series of National Academies' Computer Science and Technology Board reports over the past several decades³.

³ Computer Science and Technology Board, National Academies of Science, Engineering, and Medicine, Foundational Science for Cybersecurity, final report, 2017. See also NIST's Special Publication 800-160, Computer Security Resource (Nov. 2016; https://doi.org/10.6028/NIST.SP.800-160)

Some IoT devices will have simple applications running on bare metal, that is, without general-purpose operating systems. Other "Things" might need simple operating systems focusing just on specialized requirements such as real-time guarantees, while yet others may require full-fledged operating systems. Thus, scalable hardware and software are likely to be useful for economic reasons and operational effectiveness. Implementations are likely to range from micro-operating systems on small processors to larger reprogrammable environments for centralized Control of Things for entire enterprises.

Similarly, a range of development support is needed – from totally embedded as-delivered hardware with no possibility of software changes (except perhaps for recalls and possible remote updates) up to "Things" with flexible development environments and programming-language support. Thus, programming languages and compilers might need to encompass the very simple and the much more complex. Concerns for greater trustworthiness will be important, especially for embedding potentially unsecure applications into a nevertheless trustworthy environment.

Users generally lack expertise and patience, have limited ability to cope with complexity, and are unaware of corner cases. Consequently, the design and implementation of user interfaces for "Things" and their controllers will require special attention and care. These interfaces need to be seamlessly easy to use, intuitively self-evident, and friendly for those who are technologically impaired, as well as adequately configurable by everyone.

Especially problematic are easily managed "Things" that exist today (conventional light bulbs, toasters, and so on) whose computerization might render them completely unusable when they fail. Even worse might be mechanically failsafe devices today that might no longer work manually. One such example might be a fully automated automobile whose doors cannot be opened from the inside if the battery dies or the car is under water, or perhaps a refrigerator door that cannot be opened because its *Thing* controller has crashed – or been hacked. Fail-sensible techniques will be essential.

The needs for seamless installation and integration are critical from the customers' viewpoint, but this should not be a motivation for ignoring security. One of the major risks here is the prevailing quest for simplicity – for example, just barely meeting the bar for compliance with standards and expectations, as well as poorly addressing needs for ease of installation and ease of use. Standards are needed to facilitate interoperable installations involving many different vendors' devices. Connection protocols should not be as simplistic and unsecure as they often are today.

Any local networks within a home or enterprise must be suitably isolated from the Internet and other outside connections – except where interactions are explicitly desired and adequate protection can be assured. Certain systems and "Things" will to some extent have to be resilient and resistant to insider misuse, although that may be less important to friendly homes than corporate entities.

On the other hand, Internet firewalls must be much more impervious to outsider misuse than today. Ideally, fixed passwords and default encryption keys should be eschewed in devices – although they are far too common today, and indeed were exploited by the Mirai malware (as noted previously). Nevertheless, there will be cases where trustworthy updates cannot be achieved and recalls might be the only alternative. To enforce recalls, firewalls may need to recognize traffic from recalled and/or compromised "Things" and block the communication to protect systems on the rest of the Internet.

Also, we must consider needs for oversight, consumer protection, regulation, and liability for flagrant violations that result in serious risks. As software makes its rapid transfer into our physical world through "smart" "Things", we cannot afford to simply transfer the notion that software tends to be provided "as is" – without liability for the consequences of flaws. Electronic products that have the potential to hurt or kill people are typically subject to some form of government regulation and testing to protect consumers.

When the safe operation of a product is dependent on its software being secure and reliable, regulation will need to address those aspects of product safety. Also, the responsibilities of everyone involved need to be established and made clear. For example, if your home burns down because of a hacking attack on your IoT installation, or your negligence in failing to protect your technological devices, could your insurance companies deny coverage for known but unaddressed vulnerabilities, or even preexisting conditions?

In summary, we will need some meaningfully trustworthy hardware and software components, and much better development and deployment practices than we have at present – to enable the IoT to provide adequate human safety, security, reliability, usability, and satisfied users.

Some Specific Efforts

It is highly desirable to study a few types of "Things" as developing prototypes in research and development and attempt to ensure that all reasonable risks have at least been addressed. We would benefit from a few very successful cases to pave the way for how this could be done in the future. The combination of system engineering, hardware and software engineering, and careful application development – perhaps with some formal analyses to provide better assurance – would be extremely valuable to everyone else competing in the IoT marketplace.

Thus, a few well-designed, well-developed, and trustworthy systems that are well documented would provide wonderful examples for other developers. A step in that direction is the documented example of principled security design for a fictitious wearable fitness tracking system that was produced by the IEEE's Center for Secure Design under the auspices of the IEEE Cybersecurity Initiative⁴.

It would also be very important to provide developers with the tools and knowledge to build security, privacy, reliability, and other aspects of trustworthiness into the systems that they build. This is particularly important for developers of IoT systems who may have even less security expertise than traditional software developers. We have recognized this need and are involved in several efforts to address the situation – including the new IEEE Cybersecurity Development Conference (IEEE SecDev) and a strategic independent R&D initiative at SRI International on IoT security and privacy.

Some Thoughts for the Future

Today's population displays a wide range when it comes to understanding computer technology, ability to use it, and to have access to it. We can't deny access to essential services to portions of the population by ignoring their inability to correctly use certain technologies. Above all, we have serious needs for better computer literacy in the entire population. Many of the risks and needs discussed here are not just specific to the Internet of Things and have commonalities with more general uses of computers.

⁴ J. West, et al. WearFit: Security Design Analysis of a Wearable Fitness Tracker, February 2016, http:// cybersecurity.ieee.org/blog/2016/02/17/wearfitsecurity-design-analysis-of-a-wearable-fitness-tracker/

However, we must also consider self-driving vehicles as "Things" in the evolving automated highways, as well as automated airplanes – and treat them similarly in the same basic context. The very concept of the IoT brings us to a much more personal and visceral focus in its manifestations in homes, vehicles, and wearables, and in that sense, it touches everyone to some extent. Even those who are unwilling may eventually be forced to buy IoT-enabled appliances, simply because there are no longer any alternatives.

Today's supposedly sage advice about how to deal with safety and security needs to be significantly upgraded. For example, while we are familiar with admonitions such the following, not everyone follows them: Beware of social engineering, hucksters, and easy solutions! Don't click on suspicious links! Don't display your most personal information on social media! Adhere to (or better yet, exceed) best practices for security! The new risks will be much more pervasive, and we will need to determine what reasonable caution and common sense will look like in the world of the IoT.

Indeed, the IoT is likely to become very contentious unless serious coordinated efforts are made proactively by governments, standards committees, purveyors of "Things" and "Thing" infrastructures (including the Internet itself) and user communities. For considerable further background, see recent testimony before the U.S. Congress.⁵ Also, some so-called best practices are considered in recommendations from the Department of Homeland Security11 and BITAG.⁶ However, best practices are generally nowhere near good enough.

The prospect of billions of sensor-equipped and Internet-connected IoT devices would be tempting to any organization that wants to collect information for intelligence or evidence, or to exploit the devices for propagating DDoS attacks, or other nefarious purposes. The risks of dumbing down cybersecurity and cryptography for such purposes would be enormous – especially with respect to the IoT. There is much more on this topic than could be written here. Overall, there are no easy answers, but the time to begin asking the incisive questions is now.

Conclusion

We have described problems and potential risks that are associated with the evolving Internet of "Things". It remains to be seen whether the IoT and its "Things" can burgeon (grow and flourish, as the way of the future), or sturgeon (sometimes surviving competitively for up to two decades if not caught), or be more like the female salmon (with very short lives once they spawn). In any case, we need much more than a surgeon to fix things (and "Things"). Incremental change is not likely to succeed (indeed, it has been ineffective for so many years), and some sort of radical change may be needed.

⁵ K. Fu, Infrastructure Disruption: Internet of "Things" Security, Testimony before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing, and Trade, November 2016, https://energycommerce.house.gov/hearingsand-votes/hearings/understanding-role-connected-devicesrecent-cyber-attacks and York, K. Dyn Statement on 10/21/2016 DDoS Attack (Oct. 22, 2016); http://dyn.com/blog/dyn-statementon-10212016-ddos-attack/

⁶ Internet of Things (IoT) Security and Privacy Recommendations, BITAG Broadband Internet Technical Advisory Group, November 2016: http://www.bitag.org/documents/BITAG_Report_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Behavioral Influences in Cybersecurity

The challenge of cybersecurity is an almost existentially difficult one. Virtually all information technology assets share connections and data across multiple users and organizations, and often across international borders. Billions of individuals and millions of organizations use the public internet to access a truly countless number of connected devices and vast amounts of data. These trends are bringing the virtual and tangible worlds together into cyber physical systems that extend the risk of cybersecurity attack into the everyday world in which people work, live, and play.

As the scope of the cybersecurity challenge has grown, so has the range and diversity of potential solutions. Once viewed as a merely technical problem marked by the seesaw escalation in capabilities by those who would attack and defend the nation's information systems and critical infrastructure, cybersecurity now enjoys the attention of economists and other social scientists exploring the role played by human decision making in effective security.

The study of human cognitive biases in particular represents an area of research with great promise to improve cybersecurity, though to date it is a largely untapped one. The growing understanding of how cognitive biases affect decision making is being used to influence behavior in a wide range of areas outside of cybersecurity, including public health, crime prevention, financial decision making, energy efficiency, tax collection, and sports management, among many others. Cybersecurity has only recently begun to attract the attention of behavioral scientists, yet it is a topic rife with the sort of complexities that behavioral insights help address.

Going forward it will be essential for public policymakers and private business leaders to understand how a large, distributed, and diverse set of actors make decisions about cybersecurity, and how systematic biases in human cognition affect cybersecurity behavior and investment. Policymakers in particular would do well to examine, accommodate, and where appropriate, exploit the presence of cognitive biases in considering policies and incentives aimed at improving cybersecurity decision making.

From Rational to Behavioral

Early work to understand decision making in the context of cybersecurity framed choices in terms of marginal economic costs and benefits analysis, and focused exclusively on investment in cybersecurity measures by firms. Over time research has expanded to include attention to the decisions individuals made with respect to their own data privacy and online conduct. Given its unit of analysis – the individual – this newer work is inherently more behaviorally focused and serves to highlight the impact of cognitive biases and their influence on behavior.

We've learned, for example, that when online people are less likely to behave offensively when their actual identities are revealed and are more likely to divulge sensitive information when they believe others have done so. Both findings are examples of a cognitive bias in favour of emulating or trying to please peers (referred to as peer influence). Other research shows that decisions regarding privacy settings can be influenced by how choices are framed within the larger set of personal device settings, highlighting what researchers call an anchoring bias.

Peer influence and anchoring are just two examples of a diverse set of cognitive biases affecting human behavior and decision making, which also includes the phenomena of loss aversion, representativeness, and choice cost, among others. Peer Influence results in susceptibility to peer pressure and also leads people to rely on peers as sources of low-cost information about how to choose or behave.

Anchoring bias causes people to weight recent information, experience, and stimuli more heavily than older experience. Because of loss aversion, people are risk averse when faced with experiencing possible losses, and risk accepting when faced with possible gains, independent of expectations for realized outcome levels.

Representativeness causes people to draw incorrect conclusions about causation and distribution because of the tendency to view outliers, or inferences drawn from small sample sizes, as representative of system or population level phenomena. And choice cost tells us that the process of choosing can be quite difficult, and that people will often make choices in a way that minimizes the effort in making the choice, with little or no consideration of the value of different outcomes.

Our understanding of how these biases work rests on an established body of accumulated insight into human behavior gained from a variety of disciplines, including psychology, sociology, and neuroscience. This body of applied research is often collectively referred to as *Behavioral Economics*, and its origins can be traced to Nobel Prize winner Herbert Simon's seminal research in the 1950s in which he argued what now seems obvious, that humans have access neither to unlimited knowledge nor to unlimited information-processing capabilities.

What makes our growing understanding of human cognitive biases so promising a tool for informing research and policy in the field of cybersecurity is the magnitude of the effects biases can have on actual behavior and its track record of success in real world applications outside of cybersecurity. A well-known experiment conducted with MBA students demonstrates the power of bias. Researchers gave two groups of students the same bottle of wine and asked them to estimate a fair price for it. Prior to doing so the students were asked to recall the last two digits of their Social Security Number (SSN). The recall exercise was portrayed to participants merely as a means to separate students into two groups. In fact, it was a way to subconsciously anchor students on a set of low numbers (00-49) and high numbers (50-99). On average, the students with SSNs ending in high numbers were willing to pay remarkable 72% more than those whose SSNs ended in low numbers.

One's SSN should, we would expect, have absolutely no bearing on our estimations of the price of wine. Yet the subtle introduction to the subjects that some of them were in the "low number" group and the rest in the "high number" group was enough to dramatically affect (anchor) value estimates. Other research shows that it is not just graduate students in artificial test environments who are affected by cognitive biases, but everyone, including highly educated and experienced experts, such as judges and doctors.

How might these biases come into play in the context of cybersecurity? A team of researchers in the United Kingdom and Germany experimentally examined whether cybersecurity professionals' probability perceptions are susceptible to anchoring. The researchers' experiment asked two groups of participants, cybersecurity professionals and ones drawn from the general public, to indicate willingness to pay to avoid various hypothetical "negative lotteries" – lotteries that always result in losses, but of uncertain amounts. While there were systematic differences between security professional and general public responses, security professionals were found to be as susceptible to the anchoring bias as were members of the general public. Other work by researchers at the University of New Mexico and Lawrence Berkeley National Laboratory indicates that neither the frequency nor magnitude of U.S. data breaches increased from 2005 to 2015, contrary to public perceptions. It would be interesting to track cybersecurity experts' estimates of cyber risk over time, and measure how these estimates are influenced by (anchored to) external stimuli, for example the occurrence of and significant media attention to high profile breaches.

Tracking the same estimates for senior business executives (e.g. CEOs and CFOs) would be equally interesting. Economic theory tells us that executives will underinvest in security because of its public good nature, but it's unclear how executives establish their implicit estimates for the chance and cost of breaches and what variables anchor these estimates. A team of researchers at the University of Maryland has shown how executive views of cybersecurity evolve over time, and that large companies tend to defer major cybersecurity investments until a major breach happens, after which significant funds are allocated to cybersecurity. More insight into the cognitive influences on expert and executive risk evaluations would be enormously helpful to policymakers trying to encourage organizations to adopt better cybersecurity practices and make timelier cybersecurity investment.

As highlighted above, we know that people are more likely to divulge sensitive information when they believe others have done so. But the research associated with this finding has focused on what people do with their own personal data. We don't yet know how or how much this behavior translates to organizational contexts in which people work either as executive decision makers or in operational roles as stewards of an organization's sensitive data or critical infrastructure. Better understanding of this translation would be invaluable to those trying to understand the decisions and behavior involved on the defender side of breaches, and to develop strategies by which they may be prevented.

Consider the case of password sharing in professional environments. Cost-benefit analysis tells us that sharing bears a high potential cost (severe employer or possibly even legal sanctions if the password sharing is discovered) relative to whatever benefit may accrue from sharing. Yet it is reasonable to assume that the peer influences that affect people's private lives affect their professional behavior too. After all, in real life password sharing is common. Corporate passwords are shared because prospective borrowers (peer influencers) are persistent. They may claim a real or contrived emergency need for a password, for example, and convince their colleagues to ignore their internal cost-benefit analysis.

Another way in which cost-benefit analyses can be stymied is via the effect of choice cost. Mathematically we know that expanding choice (i.e. relaxing constraints), improves outcomes for any constrained optimization problem. This is the principle behind such policies as cap-and-trade emissions markets. Central authorities cap total emissions at a national level and set initial individual emitter limits, but then let emitters trade emission rights that allow initial individual limits to be exceeded. Market participants determine among themselves how the system-level emission targets will be met, based on individual comparative advantage. But cognitively we know that the process of assessing and deciding between multiple options requires effort, and often leads to heuristics that minimize the amount of active option analysis that must be performed.

The presence of choice cost underlies the concept of choice architecture, the deliberate design of the environments in which people make choices, to improve the ease and quality of choices. Good choice architecture reduces the number and complexity of decisions people need to make to accomplish a task, and also provide effective default choice options. A good example of choice architecture and the use of effective defaults, one found outside of cyber-security, is retirement plan offerings. An employer-sponsored plan with 20 fund offerings has over a million combinations of fund selections, one with 30 plans over a billion combinations, and one with 40 over a trillion – clearly far more combinations any person could independently assess in the context of their personal retirement situation.

Acknowledging this problem, the financial services industry has created default fund selections linked to participants' targeted retirement date, eliminating the need for analysis and providing low-choice-cost defaults which are genuinely good choices for savers. Importantly, the introduction of retirement date-based funds has led to increased plan participation. The success of these funds, and of choice architecture applied to a wide range of decision environments, suggests there may be circumstances in which it is better to constrain choice rather than allow for greater flexibility in meeting specific cybersecurity standards.

How might choice cost come into play in cybersecurity? The voluntary Cybersecurity Framework created by the National Institute of Standards and Technology (NIST) – see below – divides cybersecurity into five functions correlated to the cybersecurity risk management lifecycle: Identify, Protect, Detect, Respond, Recover. Other complementary analyses propose additional dimensions by which to further segment cybersecurity functions. For example, an approach advanced by Sounil Yu, focuses on five asset classes: Devices, Applications, Networks, Data, People. This approach implies a five-by-five (or 25 cell) matrix of asset category by function, each cell potentially addressed by multiple cybersecurity options. This matrix must be considered not only for the enterprise, but also for its employees, customers, vendors, partners, and threat actors. Many factors influence choices around these multitudinous options, including obvious market forces, but the existence of cost choice suggests these choices could benefit from implementation of defaults.

The processes of translating behavioral research insights into the cybersecurity context and addressing questions like those raised above are still in their infancy. It seems a reasonable proposition to claim that when the root cause of a cybersecurity vulnerability is behavioral in nature, a part of its solution will be as well. As already indicated, almost all current cybersecurity behavioral research considers individual choices regarding privacy and how people treat their own personal data; it does not address behavior in formal organizational settings. Neither does this research often focus on organizations as the unit of analysis, though emerging research with this emphasis has been quite revealing.

Recent research shows organizations to be as subject to the same "psychological" biases as are people. For example, organizations are more likely to reduce spam when spam levels are publicly reported but tend to do less to reduce spam when the worst-reported offender produces a greater absolute level of unwanted mail, thus making other firms appear less abusive in comparison. This is not surprising – after all, organizations are merely coordinated collections of individuals, and organizational decisions are made, ultimately, by people.

In work that SRI has done for the U.S. Department of Homeland Security (DHS), we have identified a range of cybersecurity research areas for which a behavior focus could add considerable insight. DHS has played a central role in responding to two cybersecurity-related federal policy directives issued in February of 2013 by President Obama: Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*; and Presidential Policy Directive

21, *Critical Infrastructure Security and Resilience*. These directives called for NIST to create the voluntary Cybersecurity Framework mentioned above, and a working group representing DHS and the Departments of Treasury and Commerce to focus on the topic of incentives in cybersecurity.

The NIST framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The working group's work now lives on as the Critical Infrastructure Cyber Community Voluntary Program (C3VP), which supports owners and operators of critical infrastructure; academia; federal, state, and local governments; and business in their use of the NIST Framework.

One of the initial working group's primary tasks was the development of a decision model designed to assess the likelihood that information asset owners and operators will adopt the NIST Framework. That effort adopts a purely microeconomic approach, framing incentives in cybersecurity almost entirely in terms of marginal economic costs and benefits. Much like the early research into cybersecurity decision making, which has a similar focus, the working group's effort provides a foundation for exploring the influences on decision making. In the real world, however, people and organizations are often plagued by scarce, missing, inaccurate, incomplete, and just plain false data. When faced with such information challenges, widespread biases in human cognition can play as much a role in decision making as rational calculation.

In fact, empirical data show that in many situations human cognitive biases overwhelm our analytical faculties. It's hard to imagine a real world setting in which information is less available and reliable than cybersecurity. And as corporate password sharing indicates, even when there is potential to make good decisions based on reliable cost-benefit information, there is no guarantee that good decisions are in fact made. Such is the impact of human cognitive biases on decision making.

The table below poses a number of research questions involving behavioral aspects of cybersecurity, including explicit examination of the effects of human behavior and the cognitive biases that affect behavior. These research questions emphasize improving our understanding of real behavior in real-world cybersecurity situations. The questions enumerated below, organized into nine research areas, do not comprise a comprehensive set. Rather they are representative of questions whose answers promise to help policymakers improve the security and resilience of the nation's information systems and critical infrastructure and help infrastructure owners and operators understand and counter the risks posed to their infrastructure.

Some research questions are addressable in the short term and have a fairly applied orientation. Others require more fundamental evaluations of human and organizational behavior, and therefore have a more long-term focus. This distinction is at best a general guide, as there may be short- and long-term paths of research for many of the individual questions posed. The last area – data collection – is cross-cutting and has implications for research in each of the other eight areas.

Table	V1	Research	questions	involving	hehavioral	aspects	of cybersed	mrity
raute	۷.1.	Research	questions	mooring	Denaviorai	aspects	of cyberset	Juinty

	Research Areas	Example Priority Questions					
1.	Current patterns of investment in cybersecurity	How do organizations evaluate the return on investment (ROI) on cyber- security, and what ROIs are being realized in practice? How do cognitive biases such as peer influence, anchoring, loss aver- sion, and representativeness affect executive decisions about the level of cybersecurity risk organizations face, and their subsequent ROI estima- tions and investment decisions regarding cybersecurity?					
2.	The impact of market forces on cybersecurity investment and behavior at firms	How do customer reactions to breaches, and the extent to which they are negatively impacted by such breaches, affect firm security investment and behavior? How do market forces affect innovation incentives among cybersecurity providers? What cognitive biases prevalent among marketplace participants (con- sumers or corporations) skew market incentives and dynamics?					
3.	Information and asset stewards	How does choice cost impact the cybersecurity decisions? How do individuals behave differently with respect to cybersecurity when they are responsible for data belonging to others? What behavioral mechanisms that affect personal cybersecurity behavior (e.g. the inability to hide one's identity) affect cybersecurity behavior in a professional context?					
4.	Insider Threats	What incentives distinguish true insider threat activity from run-of-the- mill poor cybersecurity hygiene by employees?Why have most insider-threat mitigation strategies focused on procedural mechanisms such as training, password and account management, and activity monitoring?How are organizational perceptions of the level of insider risk determined, and to what extent are these estimates being anchored (cognitively) by factors that lead to less accurate threat assessments?					
5.	The role of trust in cybersecurity behavior	How do organizations evaluate the trustworthiness of individuals with ac- cess to information technology and industrial control systems, and where and why do these evaluations fail? How are perceptions of trustworthiness affected, accurately or inaccu- rately, by cognitive biases?					
6.	Drivers of organi- zational cyberse- curity behavior	How do the characteristics of organizations, such as mission, leadership characteristics, degree of hierarchy, innovativeness, etc., affect decisions and behavior regarding cybersecurity? How do behavioral factors at the individual level aggregate to impact de- cisions and behaviors at the organizational level? What measurable biases do organizations exhibit in their decision mak- ing, and what are the drivers of these biases?					

7.	Cybercriminal behavior & incen- tives	What incentive differences are there for cybercrime that is motivated by financial gain (economic incentives), vandalism (behavioral incentives), and political/military goals (political incentives), and what implications do these differences have for protecting critical infrastructure? What cognitive biases affect cybercriminal behavior, and how can understanding of these biases be used to combat cybercriminal behavior?
8.	Cyberinsurance	What role can public policy play in reducing information asymmetries believed to be likely in potential cyberinsurance markets? How do cognitive biases among insurance buyers, insurers, and regula- tors affect the acquisition, pricing, availability, and regulation of cyber- insurance?
9.	Cybersecurity data collection	 What lessons are there from other policy domains, e.g. the Sarbanes– Oxley Act and financial disclosure, in collecting cybersecurity related data? What policy mechanisms could encourage or mandate practical cyber- security information sharing and discloser? What behavioral mechanisms can be used to encourage greater data sharing within the cybersecurity community?

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Conducting research on how organizations and people behave in their official capacity faces obvious practical challenges, but we believe these can be done. Recent research by the Delft University of Technology and Southern Methodist University supports this view. The team of researchers was able to examine experimentally how actual information resource owners respond to notifications of abuse on their systems, looking at, among other things, how notifier reputation affects decisions to remedy abuse.

Along with the research agenda we have developed a notional research experiment intended to serve as a proof-of-concept project to demonstrate the usefulness of behavioralfocused cybersecurity research and help bootstrap a broader set of similarly focused research activities. The planned experiment will focus on evaluating how the cybersecurity investment decisions of executives at small and medium businesses (SMBs) are affected by behavioral influences. Essential to the experiment's final design is its examination of actual corporate decisions about cybersecurity and the inclusion of behavioral factors in the experiment's treatment groups. We hypothesize that we will find real-world cybersecurity decisions to be directly and consequentially influenced by playing on the cognitive biases of executives, and consider the prospective experiment to be representative of the type of applied research done in as close to real-world situations as possible that would be extremely useful in cybersecurity.

As more and more of our world – our private data, our physical devices, our critical infrastructure – is made accessible by electronic means, the threat of breaches will continue to grow. If we are to move beyond the technological arms race between cybercriminals and cyber defenders, the challenge of investing in the implementation and deployment of cybersecurity needs to be tackled with new and innovative approaches. In this paper we make the case for one such approach: understanding the fundamental cognitive biases influencing all human behavior and decision making. Doing so promises to offer useful insights on how public policy makers and private business leaders can influence behavior, by good actors and bad, to the benefit of everyone.

Enterprise Security Solutions

In this section, solutions developed by SRI and by spin-offs from SRI are reviewed. The goal is to provide a deeper understanding of the possibilities of these kinds of technology. The specific needs of any particular enterprise will vary in important ways, and the kinds of solutions outlined below can only be adapted to those needs with considerable care. While the information below provides very useful perspective on the capabilities that now exist to support large enterprises as they adopt new technologies, these capabilities should be considered only in light of a wide ranging and expert needs assessment.

To that end, SRI International offers professional services through risk assessment and threat modelling workshops. These activities could include:

- Facilitated session and/or subject matter expert speakers
- Detailed assessment report and presentation
- Business resiliency plan
- Plan for cybersecurity talent development and environmental, social and governance (ESG) innovation strategy
- Strategic game plan to prioritize advanced Trustworthy System Capability and Platform development projects
- · Incident Response Planning, Resiliency, and Business Impact Assessment Workshops
- System Security Assessment and Planning Workshops
- Agile, Risk-aware, Digital Business Planning and Partnerships

Securing Networks, Platforms, and Data

Our modern society needs trustworthy, reliable, and resilient computing systems and networks that can be operated in ways that meet requirements for security and privacy. Tools play a critical role in the development and operation of technology, and the field of cybersecurity is no exception. Those who build new systems need tools to make sure that the systems they build are secure; those who manage systems and networks need the right tools to effectively defend against attackers who are cunning, relentless, and persistent. Tools are also needed to track and analyse the provenance of the data that we rely on to make important decisions.

SRI International continues to work on Douglas Engelbart's vision of the most urgent and important problem for humanity: to improve our collective ability to solve urgent and important problems. In pursuit of this vision, researchers at SRI conduct world-leading research into the fundamentals of trustworthy computing and develop entirely new tools and methods for building security into computing platforms, protecting users, securing data, and defending computer networks. Security technologies that are the result of our research are widely deployed and currently protecting millions of users.

If you were to take a clean-slate approach to developing hardware and software for a meaningfully trustworthy system, what would you do differently?

SRI and the University of Cambridge Computer Lab have developed a clean-slate hardware-software design and implementation that is aimed specifically at security, resilience, and dynamic adaptability. The resulting CHERI (Capability Hardware Enhanced RISC Instructions) system has the ability to run potentially untrustworthy software in a constrained compartment in which the software can do no harm. CHERI enables the development of secure components on which to build trustworthy applications.

The CHERI processor instruction-set architecture (ISA) has the ability to efficiently support least-privilege access controls, efficient domain switching, and compartmentalization [Woodruff14]. We have developed a running version of the processor on field-programmable gate arrays (FPGAs). This processor is specified in a formally-based language, Bluespec, which greatly enhances the flexible evolution of the hardware and software. Once the CHERI processor was developed, the FreeBSD operating system was run successfully within six months.

How could successful compromises of hosts in your network be detected by observing how the internal hosts communicate with external entities?

Advanced malware infections turn infected host computers into remote-controlled "bots" for use as footholds into enterprise networks or as components in botnets that can be used for a variety of criminal activities, such as denial-of-service attacks or sending spam. To enable enterprise-wide detection of such infections, SRI developed BotHunter, a tool that monitors the two-way communication flows between hosts within an internal network and the Internet. BotHunter helps network administrators by rapidly identifying infected machines inside the network that are clearly and helplessly under the control of external malicious hackers. BotHunter is based on a dialog correlation algorithm. The system monitors network dialog patterns and correlates them to a model of events that typify malware infection. The application creates a summarized alert when a suspected infection is found, and includes an auto-update service to recognize emerging threats.

SRI developed a series of BotHunter prototype applications for Windows and Unix (Linux, MacOS) that were made available for free download starting in 2007. More than 400,000 users have downloaded the free software releases of BotHunter. The technology has been licensed to TaaSera Inc. and MetaFlows Inc. who provide commercial enterprise versions of the BotHunter technology (see below for more information on BotHunter).

How could human-machine interfaces be designed to make network operators much more effective and efficient in managing security information and actions?

BotHunter is the answer.

Network administrators who manage complex networks need to monitor the output from thousands of security sensors, and need to take action to respond to attacks on the network. Cognitive overload and inadequate user interfaces pose significant challenges to effective and efficient operations. Operators can be easily overwhelmed with too much detail; however, if the detail is suppressed, they may miss important trends or specific relevant events. In ongoing research, SRI has developed interfaces by partnering with companies who design modern computer games.

SRI has developed the prototype VIVID display software, which runs on SRI's bRight research prototype system that uses face recognition and gaze monitoring systems, and proximity, gesture, and touch sensors to build detailed user profiles. The VIVID display (Figure V.2) provides a three-dimensional view of cyberattacks and defenses. Designed by SRI with consultants from the computer game industry, the display shows individual machines (grouped by virtual private networks) and their current connections to external sites on a world map.

By geolocating the target of every flow arising from the protected network, the user can quickly observe all anomalous connections to geographic regions of interest. Large-scale exfiltration of data, bot-like behaviors, and system connectivity are represented visually. The overall security status of the entire protected network is displayed with a "mood ring": a background coloration and pattern. In this way, an operator can, in a single glance, get an overall impression of the cybersecurity status of the network, and visually locate any specific point of cybersecurity concern.

Figure V.2. The VIVID display of current cybersecurity status of a protected (virtual or real) private network



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

The VIVID display of current cybersecurity status of a protected (virtual or real) private network. The infected machine on the far right is represented as a structure that is on fire, with red flames erupting. Each monitored machine produces a trail of data, where the data is categorized into benign or normal data (shown in blue) or malicious data (shown as red flares dropped below subject machines). Current network flows arc up from the observed machines; normally, these arcs have a series of white pulses where the frequency, brightness, and width of the pulses along the arc indicate the network flow including bandwidth, latency, etc.

Displaying cybersecurity threat information gathered from SRI's honeynet, SRI's BotHunter tool, and other sources, our "Infected America" display in Figure V.3 shows the current sources of infection and cyberattack. The display can be adjusted to provide visual representations of subsets of the data, sliced by organization type (such as edu sites). The user can traverse the dataset geographically and zoom to a state, city, or single city block, and can traverse the dataset to view specific details of the infections that are present.

The "Infected America" display of current sources of cyber infection, as sensed by a large honeynet, deployed BotHunter sensors, and other sources. Each blue dot represents a detected source of infection. The buttons on the top right enable users to view subsets of the data collated by organization type and other dimensions. Figure V.3. The current sources of infection and cyberattack



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

How to track and map illegal activity on the so-called dark web, where traditional search engines do not reach, and how could we understand how big the unmapped portions of the Internet are?

LIGHTS (Learning and Indexing the Geography of Hidden Tor services) project uses a "dark crawler" called the Hidden Service Forum Spider, which collects content from hidden services. SRI has also developed The Tor Hidden Service Probe (HSProbe), which is a multithreaded application designed to interrogate the status of Tor hidden services and extract hidden service content. HSProbe is an HS-protocol-savvy crawler that uses protocol error codes to decide what to do when a hidden service is not reached. HSProbe tests whether specified Tor hidden services (.onion addresses) are listening on one of a range of pre-specified ports, and optionally, whether they are speaking over other specified protocols.

How can we track and analyze the provenance of data originating from multiple distributed heterogeneous sources?

SRI has developed the open source GPLv3-licensed SPADE (Support for Provenance Auditing in Distributed Environments) research prototype in projects under NSF's Software Development for Cyber Infrastructure (SDCI) and Information Integration and Informatics (III) programs. The first generation inferred provenance from filesystem and process activity, used novel overloaded namespaces⁷ to transparently transfer provenance across hosts, crypto-graphically certify provenance, and support file lineage querying and verification.

The current generation of SPADE provides a provenance kernel, control for manipulating the provenance reporters, storage databases, filters, and summarization modules. It supports file – and process-related provenance gathering on Linux, Mac OS X, Windows, and Android; integration of provenance records of long-lived TCP and UDP connections; and lets external applications send

⁷ Ashish Gehani, Dawood Tariq, Basim Baig, and Tanu Malik, *Policy-Based Integration of Provenance Metadata*, 12th IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 2011

provenance in a domain-specific language. SPADE can store records in the Neo4j graph database, any JDBC-compliant SQL relational database, and AT&T Graphviz formats. Also included are provenance aggregation filters for diverse versioning policies⁸, a fusion filter for merging provenance streams, sketches⁹ to accelerate distributed queries, and interactive querying.

How to detect APTs and other cyberattacks, which continue to become more targeted and stealthy, while most computing systems offer only minimal visibility into their inner workings?

Tagging and tracking of provenance and causality across an enterprise at scale and with flexible granularity-while maintaining a low impact on runtime performance-requires a combination of new core technologies that are integrated in a holistic fashion. TRACE combines novel host-level tracking techniques with a proven enterprise-wide tracking system; both are configurable via a high-level programmable causality plane.

TRACE aims to enable the detection and investigation of APT attacks in an enterprise environment using provenance information. Provenance captures multiple aspects of information about an entity: what the entity's origin is; how the entity is derived; and when it originated. In the context of APT defense, entities with trackable provenance information are of various granularity; they include processes, network connections, files, and data items within files. The what-provenance of an entity e is the set of other entities that have causally influenced e's value/state (e.g., if a file's content comes from a number of network connections, then its provenance contains the IDs of the corresponding sockets); whereas, the howprovenance of entity e consists of events and their causal ordering - organized as a causal graph – demonstrating how.

The goal of TRACE is to develop a practical provenance-tracking framework that captures both what- and how-provenance by leveraging the advantages of both approaches and overcoming their respective limitations. Hence, TRACE is able to execute both what-provenance and how-provenance queries. For example, given a corrupted dataset x, two what-provenance queries are: (1) "What is the source/entry point of x?" and (2) "which other files in the enterprise were derived from (and corrupted by) x?" A sample how-provenance query is: "Construct a causal graph showing the events/entities that led to the corruption of x and those that have been further corrupted by x".

TRACE aims to make currently opaque computing systems transparent by designing a highly scalable, distributed, and programmable provenance tracking and collection system for the entire enterprise network. An enterprise network often contains different host systems, subnets, and middleboxes. Therefore, it is critical to have a central coordination plane that provides uniform specification on what to track, how to track and how to map causality across entities. The programmable causality plane (PCP) provides a central view for provenance across the entire enterprise, such that global policies can be enforced. The host-level provenance tracking system monitors host execution and collects both what- and how- provenance for individual host systems. The system provides both logging and provenance propagation primitives. Both primitives feature innovative techniques that will substantially ad-

⁸ Ashish Gehani, Dawood Tariq, Basim Baig, and Tanu Malik, *Policy-Based Integration of Provenance Metadata*, 12th IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 2011

⁹ Tanu Malik, Ligia Nistor, and Ashish Gehani, *Tracking and Sketching Distributed Data Provenance*, 6th IEEE International Conference on e-Science, 2010

vance the state of the art. In particular, the unit-based logging technique selectively instruments programs such that execution can be divided into units. This approach makes causal inference much more precise, and allows to identify and garbage-collect useless events. Moreover, the novel change-impact causality (CIC) concept enables efficient and precise provenance propagation, and causality inference by first spawning multiple concurrent executions and then aligning and comparing the executions. The enterprise-wide provenance tracking system builds upon SRI's SPADE engine, which has been proven to be scalable and high-performance. The system collects provenance from individual entities such as hosts (via SPADE reporters) and constructs the distributed enterprise-wide causal graph that can be queried. SPADE provides the underlying distributed storage and processing infrastructure and presents a central view to the PCP. Hence, SPADE can issue APT-related queries regarding the whole enterprise. The execution of such queries in distributed fashion is possible through witness skeletons, a new construct that also enables verifiable consistency of provenance information by attesting to the provenance state of a particular host at a specific time. Finally, SPADE is scalable owing to extensive query caching and optimization.

Secure Critical Infrastructure

As our critical infrastructure evolves into modern, interconnected cyber physical systems, protection against cyberattacks is quickly becoming of paramount importance. Attacks against ordinary IT systems have negative consequences that we are reminded of almost daily, with stolen data used for criminal or espionage purposes. However, the consequences of similarly successful attacks against critical infrastructure or cyber physical systems could be radically worse in nature and have a direct impact on the physical world, even causing injury or death on a potentially large scale.

Challenges

It is well known that Industrial Control Systems (ICS) that support the critical infrastructure are vulnerable and have even become the targets of well-crafted ICS-specific cyberattacks. With the emergence of such cyberthreats, it becomes imperative to create efficient ICS-specific defense mechanisms that complement traditional enterprise security solutions.

Detection and Analysis of Threats to the Energy Sector (DATES)

The DATES project advanced the state of the practice in intrusion detection and situational awareness with respect to cyberattacks in energy systems, through the adaptation of detection algorithms for process systems, and the development of novel anomaly detection techniques for such systems into a detection suite. SRI International led the DATES team with its collaboration partners Sandia National Laboratories, ArcSight, Inc., and Invensys Process Systems.

The DATES solution extended the state of the practice in ICS monitoring by implementing the following:

- Multiple detection algorithms, including an ICS-aware Snort knowledge base, and also SRI's components for stateful packet inspection, probabilistic/Bayesian analysis, and event threading.
- A unique model-based detection capability, including a communication pattern anomaly detection module, which leverages the unique traffic characteristics of ICS to facilitate detection of novel attacks such as zero-day exploits.

- A non-intrusive network monitoring design based on passive listening, which employs a separate network interface for event reporting. This design makes the monitoring appliance invisible to conventional network scans and guarantees that the critical function of the ICS is not affected at all.
- Integration of the DATES monitoring components with the advanced, market-leading ArcSight SIEM Platform. The DATES components can easily be adapted to communicate with other types of event-consuming tools.

The intrusion detection framework in DATES contained multiple detection algorithms and combined conventional attack signature detection, protocol analysis, and a Bayesian component adapted from SRI's EMERALD system. These detection approaches were geared to detect attacks similar to the attacks seen in enterprise networks, as process control networks increasingly use commodity platforms such as Microsoft Windows workstations, routing and switching equipment that is logically similar to enterprise counterparts, and standard Internet protocols such as TCP/IP and HTTP/HTTPS. In addition to using intrusion detection components designed for enterprise networks, SRI employed control-system-specific monitors that perform in-depth analysis of ICS protocols (such as Modbus) and can leverage the special-purpose characteristics of process control systems to facilitate anomaly detection.

Figure V.4. Representative DATES architecture. The defended system is instrumented with detection and correlation DATES solutions to produce a situational awareness framework that is effective against ICS-specific attacks



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Figure V.4 depicts a representative architecture of the defended system, which is instrumented with the detection and correlation solutions proposed in DATES. The architecture is applicable to control systems in sectors such as electricity distribution supervisory control and data acquisition (SCADA) or an oil refinery distributed control system (DCS). SRI and our partner Sandia National Laboratories developed implementations of this architecture for our DATES development and test environments.

DATES and New ICS Sensors In to a Ready-to-Install Framework

SRI developed the DATES sensors and the new sensors as prototypes and integrated them into a standalone framework. SRI also developed an installer that allows the customer to easily set up the software on an appliance, and a simple GUI that enables interested parties to investigate the results of the detection framework.

DATES in action: a) The simple GUI for the integrated framework enables human operators to investigate the results of the detection framework (left); b) The Invensys DATES demonstration at SRI International achieved successful distributed and cross-site attack detection (right).

SRI extended DATES by designing a modular framework that integrates sensors and a new type of content-based sensor that characterizes normal command and data sequences applied at the network level, while proposing mechanisms for achieving a low false positive rate. The more recently developed sensor proposed a new probabilistic-suffix-tree-based approach for ICS anomaly detection, which extracts the normal patterns of command and data sequences from ICS communications, while reducing the false positive rate.

National Electric Sector Cybersecurity Organization Resources (NESCOR)

The need to improve the relationship between and among government and industry for cybersecurity is a constantly recurring theme. The U.S. Department of Energy (DOE) noted an exponential increase in complexity in securing an ever-growing electric grid with an increasing number of stakeholders. This complexity underscored the need to create a comprehensive public private partnership to coordinate the efforts in the industry to meet the growing challenge of securing the electric sector. Although some information was being shared, and some collaboration was taking place, it was not on a scale or with a speed commensurate to the importance of the topic.

SRI was a key member of the National Electric Sector Cybersecurity Organization Resource (NESCOR). The Electric Power Research Institute (EPRI) led this effort to strengthen the cybersecurity posture of the electric sector by helping to establish a broad-based publicprivate partnership with the DOE for collaboration and cooperation. NESCOR served as a focal point to bring together domestic and international experts, developers, and users to specify and, if applicable, test security of novel technology, architectures, and applications for the electric sector. NESCOR addressed the priorities for development of products and deliverables necessary to assist industry and government in addressing the cybersecurity challenges to electric sector reliability. Stakeholders, most prominently asset owners, worked collaboratively to identify key issues that affect Smart Grid cybersecurity, and to develop project and product concepts.

Co-Developed Products, Processes and Services Iteratively with All Stakeholders

Through our participation in NESCOR, SRI helped bring together focused sub-teams to work with stakeholder communities to develop security requirements, use cases, best practices guidelines, mitigation strategies, and training products. SRI co-led and contributed to the teams that developed cybersecurity failure scenarios and mitigations for the electric sector and security guidelines for the electric utilities, both of which are widely used by utilities within and outside the U.S. The failure scenarios and mitigations covered all the relevant systems in the electric sector: (1) Advanced Metering Infrastructure (AMI); (2) Distributed Energy Resources (DER); (3) Wide Area Monitoring, Protection, and Control (WAMPAC); (4) Electric Transportation (ET); (5) Demand Response (DR); (6) Distribution Grid Management (DGM).

Moreover, SRI was the main contributor to the strategies and guidelines for utilities that plan and implement an Integrated Security Operations Center (ISOC), which includes corporate systems, control systems, and physical security. Through iterations of development, feedback, and refinement, the NESCOR document products were improved until approved for transition to test and evaluation.

Smart Grid asset owners and operators are using NESCOR guidance in risk assessment, planning, procurement, training, tabletop exercises and security testing. Documents such as the failure scenarios, associated usage guidance, and list of common mitigations are used by utilities as they assess the cybersecurity of their control systems. For example, the California Energy Systems for the 21st Century (CES-21) program, which addresses challenges of cybersecurity and grid integration of the 21st century energy system for California, is using the NESCOR failure scenarios as a basis for its solution research and development.

Vision and Biometrics

Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristic and can be used to establish or verify personal identity of individuals. Examples of physical characteristics include face photos, fingerprints, and iris images. An example of behavioral characteristic is an individual's signature. Biometric technologies can provide higher degrees of security than other technologies employed alone.

For many years biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. However, the marketplace for biometrics solutions has widened significantly because of the rapid advance of other technologies that can be combined with biometric characteristics, in particular digital vision technologies and machine learning based on Artificial Intelligence (AI).

The ability of a machine to see is increasingly prominent because machine learning is combined with neural network systems that allow algorithms to be trained on very large quantities of data collected from a wide range of sources. Facial recognition can now build itself by learning to recognize common and unique features across a large database of facial images. While facial recognition is one of the areas where machine vision technology has really started to shine, the excitement certainly doesn't stop there, because machine vision is starting to go beyond just assessing facial characteristics.

Challenges

There exist a variety of challenges in banking, insurance, energy, and the public sector for which Biometrics, sometimes combined with AI and pervasive networks for data collection, can provide new solutions to long-standing problems. Some of the challenges suitable for biometric solutions are listed below.

Banking and Insurance

Banking and financial transactions of all kinds have relied on one of the earliest forms of biometric recognition for centuries. This is, of course, a signature. But signatures have always been subject to problems of authentication, they have often been forged. The rise of credit and debit cards allowed for the use of pin numbers for authentication. But pin numbers are not foolproof, they are typically short so users can remember them, and can be guessed, captured or stolen.

Banks themselves, and banking machines, are the subject of direct action by criminals, and while measures have been developed that increase the risks of such attempts, including video surveillance, they have tended to serve as an *ex post* deterrent. More sophisticated criminals try to impersonate customers or bank staff. The move to mobile banking applications, which customers find very convenient, have created additional security challenges. Mobile devices can be lost, stolen or hacked. A bank cannot easily be sure who has access to it.

Many of the challenges facing the insurance sector are similar to those in banking. In addition, this sector has a high exposure to fraud (false claims for injury, and medical services) and exposure to the physical security of insured property.

An important feature of these challenges is that quick, reliable authentication of individuals increases the quality of the experience for the consumer, whereas a clumsy, slow and unreliable processes frustrate consumers and this leads to insecure behaviors (writing down passwords, sharing log-in information, etc.).

Energy

The energy sector has a somewhat different set of challenges. In particular, the energy sector is very concerned with the physical security of facilities of many different kinds. Physical access has to be careful managed for enterprise staff, the staff of partners (supplychain partners, technical support services), and regulators. This traffic, made up of a diverse population, is potentially the source of a serious risk to the enterprise. Access should only be granted to people who have been accurately identified. Access often needs to be restricted in the case of especially sensitive areas within a single facility, restrictions that apply to different groups and even to different individuals. These controls need to exist for major facilities, and also (at the same level of reliability) for small, remote facilities.

Public Sector

The public sector's challenges are on a different scale. Banks and energy facilities seek to manage a relatively small stream of people into and out of their facilities. So does the public sector. However, in the case of the public sector such facilities may be very sensitive, and require very high reliability in security systems.

In addition, the public sector often seeks to manage large crowds of people, often in poorly defined public spaces. Some of these spaces, for example railway stations, represent key components of very sensitive infrastructures. Airports are more completely controlled, but the requirement to accurately and quickly identify and track people, while at the same time allowing them to move through the facility very quickly is a strict one. There is an important trade-off to be managed between the ability to reliably identify every individual (with a very low rate of false-positive identifications) and the ability to allow every individual to pass quickly through a large facility like an airport.

Managing large crowds that may include individuals seeking to avoid detection (troublemakers at a football game, undocumented travelers) is an even more significant challenge. Physical inspection of individual identity papers is very costly and time consuming, and far from foolproof in the case of subjects seeking to avoid detection by using false or stolen documents.

Solutions

Biometric and vision technologies offer solutions to the challenges outlined above that are a clear improvement over the status quo. In many cases they can be integrated into existing architectures, whether physical or technical.

Banking and Insurance

Biometric approaches maximize convenience by maximizing mobile and multimodal authentication technology to expand reach and enable flexibility while maintaining speed and accuracy. They also offer frictionless transactions. Customer experience is enhanced as banks are able to identify and verify customers quicker with biometric systems. They provide enhanced user experience and security in smartphones, ATMs, and mobile wallets. At the same time, they reduce liability & fraud. Strong authentication of employees and customers provides instant identity verification from smartphones to PCs using biometrics-secured mobile payments. This provides greater identity protection for customers and regulatory compliance for banks.

What is required as a solution is a fast, high-quality iris and face biometric capture device designed for integration into a variety of application solutions. A simple device screen collects iris and face samples, and it should be capable of being integrated with mobile devices, passport scanners, fingerprint capture devices, badge readers, and other sensors. Key components could include:

- Simultaneous dual iris
- Color and structure of face
- Enrollment, identification, verification
- Capture time < 2 seconds

Energy

Biometric and vision technologies offer solutions for multiple entry points, at a variety of heights and distances for both indoors and outside. They allowing secure access for any type of environment and weather condition. They can be combined with multiple modalities (for example two-factor authentication) to provide an extra layer of security. At the same time, they offer ease of use, with the ability to identify a person on the move with a high-throughput and contactless system without slowing down operations.

High-security, high-traffic locations require high-speed high-assurance identification. This requires a system that can positively identify up to 20 people per minute. Such a system is ideal for factories, and other industrial and commercial facilities, as well as corporate lobbies. Key components could include:

- Hands-free
- Up to 20 people per minute
- Multimodal matches both irises and face
- Expandable to support trimodal operations
- Seamless integration with existing access control systems
- Capable of verification when integrated with a credential
- Interoperable with a centralized control system and capable of supporting a scalable distributed enterprise deployment

Public Sector

For the public sector biometric and vision technologies allow for at a distance, on the move capabilities. This includes quick, convenient access to buildings and controlled spaces with multimodal and high-throughput systems, replacing existing identification cards. They can also operate in any environment or weather condition, offering the management of a more efficient and safe large-scale operational capability indoors and out.

This kind of capability should be embedded in a scalable software platform for identity management through an intuitive, easy-to-use web interface and an open, secure REST API. The platform should provide a set of core services for multimodal biometric identification, as well as a suite of auxiliary services, including component registration, health monitoring, and reporting. Key components could include:

- Multimodal multifactor identification
- Multiuser web interface
- Centralized device configuration, health monitoring, and updates
- · User-defined subject categories and alerts
- Configurable retention policy
- Single and multisensor encounters
- Rich encounter logging
- Mixed vendor matchers by modality
- Biometrically backed badge generation

Implementation: Secure Biometrics

Biometrics are becoming an increasingly popular and effective approach for identifying, authenticating, and granting access to individuals. Biometrics are heavily used by law enforcement, homeland security, intelligence, and defense communities. The objective of this paper is to highlight security and privacy issues facing current biometrics-based identification and authentication (BIA) systems. Such issues have to be solved before widespread adoption of such systems, because a breach of these systems can be devastating and compromise the privacy of hundreds of millions of individuals.

Current BIA systems acquire and process a user's biometric in the initial enrollment phase and typically store a processed version of it, called a biometric reference template, in the backend of the system (see Figure V.5). The backend in such BIA systems is typically implemented as a centralized (or distributed) database. In subsequent interactions with the system, a noisy reading of the same user's biometric is captured. Every subsequent reading is noisy due to imperfections in the input method, i.e., the sensor capturing the biometric reading, and other environmental factors. The new reading is compared to the stored biometric reference template and, if the matching is successful, the user is identified and authenticated.

Challenges

If leaked or compromised, biometrics (e.g., iris and fingerprints) that do not change much over time could enable adversaries to circumvent BIA systems and pose a serious threat to the privacy of individuals in those systems. In this type of systems, if the backend databases or the servers storing the biometric reference templates are breached or compromised, the biometrics of hundreds of thousands (or millions) of individuals are compromised and can be later used by adversaries to circumvent BIA systems.

A 2015 breach of the Office of Personnel Management (OPM) leaked 5.6 million fingerprints¹⁰ of federal workers, this event highlights the risks of backend compromises involving biometrics. The more government agencies and entities rely on BIA systems, the more serious this threat will become. We think that in the future BIA systems should be designed from the ground up to mitigate such large-scale compromises and leaks, or at least ensure that if they occur that the actual biometrics of a large number of users are not leaked. The next section outlines a solution to this problem.

Solutions

A secure approach to develop BIA systems is to use cryptography as the basis of their design. Instead of patching existing designs by encrypting biometric reference templates stored in backends and decrypting them on-the-fly to match and validate new biometric readings, the secure system generates and uses public helper data (PHD) to perform validation and recover a cryptographic key (a random number) that is tied to each individual/user in the system. A cryptographically secured system acquires and processes biometrics during the enrollment phase, using cryptographic algorithms such as Fuzzy Vaults (FV) or Fuzzy Extractors (FE), and saves PHD data to the backend. The PHD is generated using the user's biometrics and specific algorithms that guarantee that PHD does not leak any information about the biometrics and cannot be used alone to bypass the system.

Given the PHD and a reading of the biometric that was used to generate such PHD, one can recover a unique random number (a cryptographic key) used to identify and authenticate the user. Specifically, in subsequent interactions and to perform identification and authentication, the secured system acquires a noisy reading of the biometric and uses PHD to re-compute the cryptographic key corresponding to the user's biometric. The key identifies and authenticates the user, who can then be granted the corresponding privileges and access rights to the resources protected by the system, e.g., physical access to a facility, a device, or access to data, services, and/or information infrastructure.

¹⁰ https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.0d67db3857ea





Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018 Figure V.6. Identification and authentication in a cryptographically secured BIA system



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

The novelty at the heart of this new paradigm is that the PHD is independent and uniformly distributed without knowledge of the biometric, this guarantee is mathematically proven; therefore, even if the PHD is leaked, it cannot be used to reconstruct the biometric or bypass the BIA system. Once a correct biometric is supplied in a subsequent interaction with the system, it is used together with the PHD to reconstruct cryptographic keys to identify and authenticate the legitimate individual. Without the biometric, and even if the PHD is obtained by adversary, it is computationally infeasibly to produce a biometric that if coupled with the specific PHD produces a legitimate key.

BlockCIS - A Blockchain-based Cyber Insurance System

Even though the US cyber insurance market has been growing significantly in recent years, it has not yet reached the same levels and complexity as other well established insurance marketplaces for health, automobile, life, fires, etc. A recent enlightening study conducted shows that most of the current cyber insurance policies use a simple price model (flat rate or weighted base rate) based on answers to questionnaires on the customer's security posture. Such questionnaires are designed to attempt to capture an organization's general business, and systems and technical measures, policies and procedures, and compliance with a variety of laws and regulation; the filled out questionnaires are then used to compute the premium.

A significant shortcoming mentioned in the study is the "little attention given to the technical infrastructure". Only a few insurers consider the information technology and computing infrastructure, and little information (e.g., number of devices or IP addresses) is collected. In particular, it seems that such questionnaires fail to capture an accurate assessment of the infrastructure landscape and its attack surface.

Most insurers ask a few technical questions about security (e.g., the presence of an intrusion detection system or the use of encryption at rest), but little attention is given to its interdependencies with the technological environment the customer is operating in. Given the complexity of current cyber systems and the interdependencies between the infrastructure and the risks faced by insurance customers, relying only on such information seems insufficient. "Our first hypothesis is that accurate security posture information extraction for an organization is viable as long as the context in which the organization operates is also known".

The current approach based on questionnaires has another major shortcoming: it is a (predominately) static method for collecting data. The cyber landscape changes every day, new software vulnerabilities are discovered, devices believed secure one day may become a major threat because of a tweet, large amounts of information are regularly leaked, etc. "Our second hypothesis is that having the ability to continuously monitor, assess, and audit the security posture of an organization is a more appropriate (and necessary) path".

In this short article, we introduce BlockCIS, a blockchain-based cyber insurance system that aims to provide solutions to these challenges. In a nutshell, our system considers four entities: the customer, the insurer, third party services, and an auditor. All these entities will be connected via a permissioned blockchain. A permissioned blockchain is a secure private common ledger agreed on by the entities, and that securely enforces pre-specified access policies. A blockchain-based cyber insurance system has a natural incentive structure that can encourage entities seeking insurance to participate in the system: insurers can devise pre-miums tailored for a company's security posture, and the company can prove that a potential cyber incident is covered by its cyber insurance. Our system leverages the automated nature of smart contracts (on the insurer side), but is entirely decoupled from the payment aspect of the blockchain (contrary to many related work). BlockCIS is a continuous monitoring and processing cyber insurance system. Finally, we show that there are several options to ensure confidentiality and privacy of the data being collected and stored within the system, and instantiate the BlockCIS design using the Hyperledger blockchain framework.

Preliminary Considerations

A recent study by Romanosky et al. surveys the current state of the cyber insurance market, and its many shortcomings. This study shows that the security posture of customers is difficult to properly assess. Existing assessment methods are static, i.e., customers have to fill security questionnaires furnished by insurers. Such questionnaires consist of a list of questions related to information technology, management, policy, and adopted compliance practices. In particular, Romanosky et al. identify the lack of attention insurers pay to the technical infrastructure and its correlation with the risks from the broader environment the customer operates on.

The study also reveals that current premiums are computed based extremely simple formulas, e.g., flat rates, or weighted sums. In particular, the study identifies that 32% of policies use flat-rate pricing which does not offer any differentiation by firm or industry, and that 32% use a base-rate pricing multiplied by multiple variables relating to answers to the questionnaire, while the 35% of the policies took into account some information security controls and computed the premium as a weighted sums of products of factors. Finally, the survey shows that lack of data to accurately assess cyber posture and risk is a critical roadblock facing operation in cyber insurance markets.

Blockchain Basics

A blockchain is a shared ledger, maintained by several nodes without a central authority, it typically achieves consensus using a distributed (Byzantine tolerant) cryptographic protocol. The blockchain concept first appeared in the Bitcoin cryptocurrency as an immutable record of transfers, maintained collaboratively by all parties that hold and trade the currency. However, past years have witnessed profound and disruptive implications of blockchains in a wide range of settings. It is now possible to specify business logic for transactions, ranging from recording who owns which asset to executing self-enforcing and complex functions (smart contracts). Smart-contracts make it possible to distribute a business service among many parties, with potentially conflicting interests, to achieve a common goal.

There are two broad classes of blockchains, public vs permissioned (or private) blockchains. The distinction between public and permissioned blockchain is based on who is allowed to participate in the network, execute the consensus protocol, and maintain the shared ledger. Blockchains to be used in businesses will generally set up a permissioned network, and restrict who is allowed to participate in the network and transactions. This work focuses on permissioned blockchains.

Block Chain Based Cyber Insurance

We consider a setting in which the following four entities are involved (Figure V.7).

- 1. Insured: This is the entity that requires cyber insurance, e.g., a corporation, a hospital, a university. This entity owns and operates a (possibly geographically distributed) computing and networking infrastructure; such infrastructure may also involve non-local outsourced elements in the cloud.
- 2. Insurer: This is the entity providing cyber insurance for the insured. It is in their interest to accurately assess the likelihood of a cyber incident, for each of entities it insures, to adjust the premiums and other fees. Given the speed at which events occur in cyberspace, it is in the interest of the insurer to be as adaptive and as quick as possible to adjust the rate to reflect an insured entity's likelihood to suffer consequences of a breach or attack, and thus request the insurer to cover the damage.

- 3. Third Party Services: These are entities that provide very specialized services that may be hard for the insured and insurer to perform and are useful to assess the like-lihood of a cyber incident, or the damage resulting from it. One example of such a service could be one that is analyzing dark web forums and markets, and determine whether the network and systems of the insured are compromised (accounts on them being sold), or identify the latest strains of malware and exploits being sold (and what systems and software versions they affect, to be able to relate it to a specific insured entity's network/systems).
- 4. Auditor: In case of a (legal) dispute between the insurer and insured, there may be a need for a third party to investigate and audit the data on the blockchain to settle such a dispute. It could also be possible that such an industry becomes highly regulated and that there will be a need for auditors to be always involved in such a distributed system, and only randomly (or periodically) perform audits to ensure that the insurers actions and rates are consistent with the logged data and events.



Figure V.7. BlockCIS overview

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Basic Framework

The basic framework for BlockCIS is that a blockchain-based system connects the following entities: an insured entity (I), the ensurer (R), third party service providers (P), and auditors (A). A BlockCIS node is deployed in the network of each of these entities. The BlockCIS node deployed at I's network interfaces to enterprise services in the network, collects analytics, statistics, and submits reports and events to the BlockCIS system. For example, it could collect firewall logs and analyze the number of port-scans or other connection attempts that were blocked at the perimeter of I's network, it could also do the same for any deployed intrusion detection system. Figure V.8. BlockCIS node deployed at an insured entity's network



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018 Figure V.9. BlockCIS node deployed at the insurer's side



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018 Figure V.10. Third party services involvement in BlockCIS



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Incentives

A blockchain-based cyber insurance system has a natural incentive structure that can encourage entities seeking insurance to participate in the system. Assume company C is seeking cyber insurance from insurer R. Further, assume that R has deployed a BlockCIS-like insurance infrastructure. It is in R's interest to assess the possibility of C being the target of a successful cyber incident (e.g., attack or breach) as accurately as possible to reflect it in the premium and fees that it charges. It is in C's interest to be adequately covered if any incident occurs and also to be paying the minimal premiums and other charges to save money. R can offer C a lower premium if C deploys a BlockCIS node on its network, such a node will act as a monitor of the state of the network, and to (continuously) determine whether C is following best practices, and has its network and software adequately secured and updated. R will receive (and securely log) this information using BlockCIS.

Confidentiality

Competing business interests may require the data stored in the ledger by different parties (and most notably, the enterprise data) to remain private, even in a permissioned network. In this section, we propose three approaches that achieve different notions of confidentiality, and can be instantiated in a same permissioned network.

- 1. Private Channels: We propose the use of private channels within the permissioned network. Those channels are restricted messaging paths used to exchange data among specific subsets of network members. In particular, all data (including transaction, member and channel information) on a channel is invisible and inaccessible to any network members not explicitly granted access to that channel. In particular, the permissioned network would be constituted of many channels, and each transaction would be executed on a specific channel where each party must be authenticated and authorized to transact on that channel. Such a feature is available for example in the Hyperledger Fabric framework and enables any groups that require private, confidential transactions to coexist on the same permissioned network.
- 2. Selective Disclosure: In the cyber insurance usecase, access to raw (unencrypted) data may only be required at certain occurrences (e.g., when an incident occurs, or when the premium has to be recomputed). In that case, the enterprise may only want to provide selective access to data to the insurer. A possibility would therefore be to encrypt, at every time period (say, every day) the data with a different secret key, and store the encrypted data on the blockchain. It then suffices to reveal those keys to the insurer when selective decryption is required. To avoid storage of many encryption keys, we recommend to use key ratcheting (as in Signal). For example, one can use the key ki = KDF(msk; ti) at each time period _ti, where msk is a long-term secret key, and KDF is a standard key derivation function. In particular, it must hold that, given ki's for i 2 I, no information is revealed on the kj 's with j = 2 I.
- 3. Secure Computation on the Blockchain: As hinted in Section II-A, the current formulas to compute premiums are quite simple. In particular, many premiums are computed as weighted sums. As such, we suggest the approach of encrypting the enterprise data, while allowing to perform computations thereon; this is possible by using homomorphic encryption.

Design

We instantiate the BlockCIS design using the Hyperledger blockchain framework. We note that this is just one instantiation possibility, and that any similar blockchain platform may be used to instantiate Block-CIS. We chose Hyperledger because it has a large community of developers and adopters. Hyperledger is also an open source project by the Linux Foundation so our instantiation could be reproduced by others.

A. Hyperledger Basics

The Hyperledger Project1 aims at creating an enterprise-based, open-source distributed ledger framework. One of the main Hyperledger projects is Hyperledger Fabric, a blockchain framework implementation designed to support pluggable modular components implementations (consensus, membership, cryptography library). At the core of Hyperledger Fabric is the notion of chaincode smart contracts; transactions in Hyperledger Fabric are executed by those chaincodes. More precisely, the authorized peers run a consensus protocol for executing a replicated state machine accepting three types of transactions: (1) Deploy: a chaincode (representing a smart contract) is installed on the peers and ready to be invoked; (2) Invoke: invokes a transaction of a particular chaincode which may read and write entries in its state accordingly; and (3) Query: returns an entry of the state directly from reading the peer's persistent state.

To simplify application development on top of the Hyperledger Fabric blockchain infrastructure, a set of collaboration tools for building blockchain business networks, called Hyperledger Composer, is being incubated in the Hyperledger Project. To digitize business networks, it then suffices to define a business network that consists of:

- Assets: define the assets that are exchanged in a blockchain-based use case
- Transaction logic: define the executable transaction processor functions; the transaction processor functions will run on a Hyperledger Fabric and have access to the asset registries that are stored in the world state of the Hyperledger Fabric blockchain
- Participants: define the participants and access controls for what roles exist and which roles can execute which types of transactions

The files modeling the assets, participants, and transactions are typically created by business analysts, while the files implementing the business requirements provided by business analysts are typically created by developers in javascript. In what follows, we define an example business network for cyber insurance.

B. BlockCIS Instantiation with Hyperledger

- 1. Participants: The participants defined in our Hyperledger instantiation of BlockCIS are listed, with their corresponding roles, in Table I.
- 2. Assets: The assets defined in our Hyperledger instantiation of BlockCIS are listed in Table II. For each asset, we also describe who is expected to write/read it.
- 3. Transactions: The transactions that the participants can perform on assets are listed below. Essentially, each asset identified in Table II has a set/get transaction. The set and get operations are only accessible to participants with proper access rights defined in Access Control List (ACL) paragraph below.
 - a. Set Transactions: allow participants to modify the value of a specific asset. Our rationale to perform updates to assets through transactions is to keep an immutable log of which asset was changed when, and by which participant; such a log enables faithful recreation of any computation (after an incident for forensics purposes for example) that was performed in real time to assess the exposure/vulnerability level of an organization, and thus the associated level of risk, which would also affect the risk estimation and thus adaptive insurance rates (if used).

- b. Get Transactions: allow participants to retrieve the value of a specific asset. Our rationale to require a transaction to retrieve assets is to keep an immutable log of which assets were read by which participants, as it may affect premiums or insurance decisions, especially by the insurers.
- c. Transaction to Compute/Update Cyber Risk Score: allows participants (especially insurers) to compute latest cyber risk score based on the most recent values of the assets listed above. Many possibilities exist to compute cyber risk scores. For example, the Common Weakness Scoring System (CWSS) developed by MITRE standardizes the approach for characterizing weaknesses, and the Security Score Card3 start-up proposes a system to characterize the security posture of organizations. Recently, BinaryEdge proposed an openframework for computing scoring and premiums for cyber insurances.
- d. Access Control Rules: Table II shows the read/write access rights for each asset. Our rationalefor the current design is that most assets can be read by most participants, but write access is much more restrictive (obviously write access to an asset implicitly grants read access to it). For example, all the assets that are internal to an insured entity can only be edited by the AgentSysAdmin participant which acts on behalf of the insured entity. The DarkWebMonitor is the only one that can edit the corresponding asset DarkWeb. The CyberRiskScore can only be computed by the InsuranceBroker and is only visible to it and the AgentSysAdmin and Auditor.
- 4. Blockchains for Insurances: Many press articles or white-papers have suggested to use blockchains for insurance purposes. Most of the blockchain uses envisioned for insurance relate to automation, and most notably, automation of payment. For example, rare events (earthquakes, trip cancellation) would automatically trigger payments according to a policy specified in a smart contract. The inherent agreement on a shared ledger also enables to automate systems to improve assets transfers and claims processing, limit fraud, enable a shared view of policy data and documentation in real-time, improve customer engagement, or reduce administrative costs.

Participant	Description			
AgentSysAdmin	This is the participant that acts on behalf of the insured company, e.g., a head SysAd- min or someone in the CSO's office.			
InsuranceBroker	This is the participant that acts on behalf of a (abstract) participant representing an insurance company			
DarkWebMonitor	This is an example of a third party service, such a service could be monitoring the dark- web for any mention or listing of information relevant to an insured organization, e.g., accounts on its servers, backdoors in its software, etc.			
PublicDataMonitor	This is another example of a third party service, such a service could be monitoring the open web for any mention or listing of information to an insured organization, e.g., newly discovered vulnerabilities in software or equipment utilized by an organization.			
Auditor	This is the participant that represents an outside entity such as a regulator for the cyber insurance industry, or auditor to ensure compliance with required laws and regulations; this could also be a law enforcement entity involved in investigation large scale security breaches/compromises or investigating a major insurance case or dispute.			

Table V.2. Participant in BlockCIS Instantiation Using Hyperledger

Source: Own elaboration

Asset	Description	Participants (write/read)		
DarkWeb	# mentions in hacker chatter, # employees credentials in DB leaks, zero-day vulnerabilities	DarkWebMonitor/Everyone		
PublicData	# issues in open-source projects, job satisfaction on employment websites (e.g., Glassdor)	PublicDataMonitor/Everyone		
ForeignDevices	# external devices connecting to company access points, metadata on the external devices' OS and browser, number of pages visited from external devices	AgentSysAdmin/Everyone		
SwAndHw	# software that needs updating, max(time since last training for 90% employees), average time of reactiveness after a software update, average age of hardware, number of unsupported software used	AgentSysAdmin/Everyone		
SocialEng	# social networks links visited, # phishing links clicked from emails	AgentSysAdmin/Everyone		
NtwkHealth	# vulnerabilities discovered in pen-testing of public exposure, # open ports, # IPs used by malware	AgentSysAdmin/Everyone		
NtwkConfig	# publicly available admin domains, # insecure ciphers in certificates, # IPs the company owns	AgentSysAdmin/Everyone		
CyberRiskScore	The computer cyber risk score	InsuranceBroker/AgentSysAdmin/ Auditor		

Table	V.3.	Assets	and	Access	Rights	in	BlockCIS	Instantiat	ion U	Jsing	Hyp	erledger	•
					-						~ .		

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Blockchains are also envisioned to transition new and existing models of insurance, such as P2P insurance and micro-insurances. While our work also uses the automation nature of smart contracts (on the insurer side), it is entirely decoupled from the payment aspect of the block-chain and is to be thought as a continuous monitoring and processing cyber insurance system. In particular, none of the literature above-mentioned mentions the continuous storage of an enterprise cyber posture as a mean to measure, monitor, and audit to enable cyber insurance.

One recent independent work proposes to modernize cyber insurance using blockchains and shares ideas with our work. In particular, BinaryEdge proposes to create a blockchain by customer to continuously monitor the changes in rate over time and uses smart-contract as a set of rules of actions that will be enforced when third party services identify potential issues with the company. In particular, the solution proposed by BinaryEdge lies in where third party services are not writing on the blockchain directly, but enable the insurer to execute smart contracts based on their data. Our work extends this work further by storing the enterprise data on the blockchain (possibly in a confidential manner) to ensure end-to end integrity and reproducibility (e.g., for audit purpose) and to enable real-time changes, when changes occur in the enterprise and third party monitoring datasets.

Conclusion & Future Work

Traditional insurance providers are slowly entering the emerging sector of cyber insurance; given the nascent state of that sector, they are using manual procedures and models which they have developed for other (physical) domains. We argue that the unique nature of cyber space, a highly interconnected and inter-dependent network of hardware and software, that operates at sub-second speeds, requires automated methods and infrastructure to be able to develop a sustainable insurance ecosystem for it.

Such an insurance infrastructure involves multiple stakeholders belonging to different entities with no trusted third party, and thus a (natively) distributed and secure system connecting them is required. To address these issues, we propose BlockCIS, a block-chain based framework for cyber insurance. We instantiate BlockCIS using the open-source Hyperledger blockchain framework, and show how such a system can implement a secure distributed infrastructure for assessing cyber risk for organizations. We also describe how some advanced features such as selective disclosure of data can be added to BlockCIS. Future work includes deploying BlockCIS in an operational environment and trying to assess how accurately the computed cyber risk score mirrors likelihood of an attack or breach.

Intrusion Detection Software

Multi-session traffic analysis (also called dialog-based correlation) is embedded in a revolutionary Intrusion Detection software tool called BotHunter. Since then, MetaFlows has significantly extended and improved such technology for commercial use. Simply put, it automatically connects the dots between security alerts involving a single internal host with multiple external hosts over time.

Traditional intrusion detection software generates alerts by reconstructing a single session between two hosts and finding known patterns that confirm security violations within that specific session. This usually results in a very high false positive rate. Important events are often missed due to the huge volume of false positive or low-priority network security events.

MetaFlows uses Multi-Session Intrusion Detection Analysis. This advanced intrusion detection technique combines multiple security events (also called dialog events) that form a typical behavior pattern for an infected host. Dialog events from each internal host are mapped and scored against an abstract Malware infection life cycle model.

When the Multi-session analysis algorithm shows that a host's dialog patterns map sufficiently close to the Malware life cycle, the host is declared infected, and an infection profile (a partial summary example is shown below) is generated to summarize all evidence about the infection.

How BotHunter Works

BotHunter is NOT an intrusion detection system, firewall, spam blocker, or antivirus tool. These tools generally don't work in helping you rid your network of malware infections. Rather, BotHunter takes a different approach. It is an entirely new network defense algorithm designed to help everyone from network administrators to individual Internet-connected PC users detect whether their systems are running coordination-centric malware (such as botnets, spambots, spyware, Trojan exfiltrators, worms, adware). It is based on an algorithm called network dialog correlation, developed under the Cyber-TA research program (http://www.cyber-ta.org), by the Computer Science Laboratory at SRI International.

BotHunter monitors the two-way communication flows between hosts within your internal network and the Internet. It aggressively classifies data exchanges that cross your network boundary as potential dialog steps in the life cycle of an ongoing malware infection. BotHunter employs Snort as a dialog event generation engine, and Snort is heavily modified and customized to conduct this dialog classification process. Dialog events are then fed directly into a separate dialog correlation engine, where BotHunter maps each host's dialog production patterns against an abstract malware infection lifecycle model. When enough evidence is acquired to declare a host infected, BotHunter produces an infection profile to summarize all evidence it has gathered regarding the infection. In short, BotHunter helps you rapidly identify infected machines inside your network that are clearly and helplessly under the control of external malicious hackers.

Dialog correlation is an algorithm that classifies each network traffic exchange that occurs across your network boundary as potential infection sequence steps that occur when a host is infected with malware. Not all network traffic events generate a dialog event. Dialog events are fed directly into a separate dialog correlation engine, where each host's individual dialog production pattern are mapped and scored against an abstract malware infection life cycle model. When the dialog correlation algorithm determines that a host's dialog production patterns maps sufficiently close to the life cycle mode, the host is declared infected, and an infection profile is generated to summarize all evidence regarding the infection.

BotHunter is funded through the Cyber-Threat Analytics research grant from the U.S. Army Research Office, and is free to all end users to help you combat malware infections. In addition, BotHunter includes an auto-update service that allows fielded systems to receive the latest threat intelligence regarding new sources for ad and spyware management, botnet control sites, backdoor and control ports, and malware-related domain name lookups. The update service also publishes new dialog analysis rules to help BotHunter recognize emerging exploits and malware communication patterns. Modern malware defenses need to be adaptive and aware of the latest strategies used by Internet malware, and BotHunter is ready to meet this challenge.

Conceptual Overview

Distinguishing a successful malware infection from the vantage point of the network egress position requires a command of the two-way dialog flow that occurs between a network's internal hosts and the Internet. While many malware infections start with an initial external-to-internal infection, malware may use a wide range of options to infect a host, including indirect host infections through email, direct exploit-based infection, or drive-by infections that are launched from malicious network servers.

Furthermore, with the growth in popularity and capability of mobile laptops, direct infection of an internal asset need not necessarily take place behind a well-administered network. Malware may inject itself into a host opportunistically from any Internet access point the hosts happens to associate, or may be executed voluntarily by a victim who inadvertently accesses a Trojan binary, multimedia file, or other infected transmission source. Regardless of how malware enters a host, once established inside the network perimeter the challenge remains to identify the infected machine and remove it from service as quickly as possible.

Capturing the full scope of a malware infection requires an ability to follow a dialog that can span several participants, including the victim host, the infection agent, the source of binary updates, the command and control server, and eventually the propagation targets of the newly infected victim. Traditional network intrusion detection systems (IDSs) typically focus on inward packet flows for signs of malicious point-to-point intrusion attempts. IDSs have the capacity to detect initial incoming intrusion attempts, and the prolific frequency with which they produce such alarms in operational networks is well documented. However, being able to distinguish a successful local host infection from the daily myriad of scans and intrusion attempts is as critical a task as any facet of network defense.

How BotHunter Analyzes Network Flows

BotHunter models an infection sequence as a composition of participants and a loosely ordered sequence of network dialog exchanges:

Infection I = <A, V, E, C, P, V', {D}>

where A = attacker, V = victim, E = egg download location, C = C&C server, P = peer-topeer coordination points, and V' = the victim's next propagation targets. $\{D\}$ represents a set of dialog sequences composed of bidirectional flows that cross the egress boundary.

BotHunter's current infection dialog set {D} provides the following detection coverage for your network:

Figure V.11. BotHunter's malware infection dialog model

Dialog Class	Dialog Event	Dialog Icon	English Description
E1[bh/rb]	Inbound Scan		<host> was the target of an inbound scan</host>
E2[rb] .	Inbound Attack	IN 👥	<host> was the target of an inbound infection attempt</host>
E2[dns]	DNS Lookup to Client Exploit		<host> performed a DNS query to a malicious host associated with client-side exploits</host>
E3[rb]	Egg Download		<host> downloaded a binary executable from an external source</host>
E4[rb]	Malware C&C		<host> appears to have exchanged command and control message with an external malware controller</host>
E4[nbr]	Russian Business Net Connection		<host> attempted to connect to a monitored Russian Business Network site</host>
E4[dns]	DNS Lookup to Botnet C&C		<host> performed a DNS query to a known malware control site</host>
E5[rb]	Outbound Attack Propagation	ουτ	<host> is conducting outbound attacks, possibly to propagate a malware infection</host>
E5[bh]	Outbound Scan		<host> may be conducting an outbound IP address sweep</host>
E6[rb]	Attack Preparation		<host> is conducting activities associated with preparing to launch an attack</host>
E7[rb]	Peer to Peer Coordination		<host> is engaged in P2P communications associated with Malware coordination</host>
E8[bh]	Malicious Outbound Scan		<host> is conducting an IP address sweep using network ports associated with malware propagation</host>
E8[rb]	Outbound to Malware Site	£.	<host> has connected to a known malware control site</host>
BotHunter's Infection Life Cycle Model

BotHunter's malware propagation model is primarily driven by an assessment of outward-bound communication flows that are indicative of behavior associated with malware coordination. Where possible, we seek to associate such outbound communication patterns with observed inbound intrusion activity. However, this latter activity is not a requirement for infection declaration. Neither are incoming scans and exploit alarms sufficient to declare a successful malware infection, as we assume that a constant stream of scan and exploit signals will be observed from the egress monitor.

Figure V.11 illustrates BotHunter's malware infection dialog model used for assessing bidirectional flows across the network boundary. BotHunter incorporate initial scan detection and exploit usage, including web-based client-side infections. Host infection is then followed by malware binary downloading, installation, and coordination (in the case of botnets, spyware, and adware infections). Next, BotHunter's infection dialog model proceeds with infection propagation, which includes activity such as scanning, exploit usage, spam propagation, and attack preparation. Finally, BotHunter recognizes malware infections when systems are observed attempting to connect to known C&C servers or other address space highly associated with malicious software control (e.g., Russian Business Network address space).



Figure V.12. BotHunter's malware infection dialog model

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Figure V.11 is not intended to provide a strict order of events, but rather captures wellestablished infection dialog patterns observed among a wide variety of malware strains. We assume that bot dialog sequence analysis must be robust to the absence of some dialog events, must comprehend multiple contributing candidates for each of the various dialog phases, and must not require strict sequencing in the order in which outbound dialog is conducted. BotHunter employs a weighted event threshold system, which captures the minimum necessary and sufficient sparse sequences of events under which an infection declaration can be triggered. BotHunter infection profiles include an overall infection confidence score, which will range from 0.8 to 3.8. The higher the score, the greater the dialog evidence trail that was used to produce the infection profile. BotHunter is capable of declaring a host infected when either of three dialog sequence combinations is observed:

Condition 1: Evidence of a local host infection, and evidence of outward malware coordination or attack propagation, or

Condition 2: At least two distinct signs of outward bot coordination, attack propagation, or attacker preparation sequences are observed.

Condition 3: Evidence that a local host has attempted to establish communication with a confirmed malware control host or drop site.

Intelligent Assistant for Customers

Intelligent virtual assistants come in many different shapes and sizes – from simple webchat boxes to carefully crafted avatars that can speak numerous languages and express a range of human emotions. They can also be deployed to fulfill a wide variety of tasks – from providing an intelligent interface to your Website's FAQ page or making your site easier to navigate, to answering complex customer queries or supporting product sales.

Virtual assistants can operate as everything from standalone search or chat windows, to a sophisticated omni-channel platform integrating data from your CRM, ERP, financial and/ or analytics systems to deliver much broader functionality, a richer customer experience, and maximum ROI.

With such a diverse range of options there can be confusion about how best to ensure that introducing one adds value to your business and your brand and the practicalities of integrating it into your contact center, information systems and customer experience. To help you, this guide provides a detailed overview of how Nuance is working with leading enterprises to deploy the Nina virtual assistant, the benefits of doing so, and how in as little as a few weeks you could create your new 'Employee of the Year' – not just for this year, but for every year.

What Is Nina?

Nina is an intelligent virtual assistant designed to deliver an intuitive, friendly and professional automated experience across multiple channels including desktop and mobile browsers, mobile apps, text messages, Facebook Messenger, SMS, smart home speakers and the IVR. Leveraging world class natural language understanding technologies, Nina is able to understand not only the words your customers speak or type, but also the intent behind their requests.

This level of intelligence streamlines engagement and allows Nina to rapidly answer questions, guide customers to products, or provide step-by-step instructions for complex activities. Sophisticated dialogue capabilities also enable Nina to engage in natural, human-like conversations that consumers are happy to engage in – whether to refine their requests, discuss next steps or complete a task.

Nina delivers a consistent experience no matter which channel a customer selects, and remains fast and easy to use, even as they move between channels. Nina increases customer satisfaction and lowers costs by creating personalized engagements that rapidly resolve individual issues. Nina can process high volumes within low cost service channels allowing live agents to focus on high-value customers and more complex interactions.

In addition, Nina is designed to provide a future-ready foundation for intelligent automation.

- Upfront targeting enables businesses to serve their consumers with the right experience at the right time. Strong branding and best practice built in, means that the targeting engine is able to decide when to offer Nina, for example when a site visitor is stuck during the checkout process.
- Sophisticated tooling allows for rapid optimization as interaction data is automatically clustered for context and fed back into the system to allow the virtual assistant to continually learn and advance to handle more complex customer engagements.
- The Nuance Digital Engagement Platform balances the benefits of machine learning with human knowledge and skill enabling trained agents to engage and curate how Nina responds when presented with unfamiliar requests, and ensuring a fast response to changing market conditions in real-time.
- Investments in Nina easily extend from one channel to another, creating both a consistent omni-channel experience and low total cost of ownership.

Nina meets the needs of large global companies with rigorous demands for seamless transition between automated and human assisted engagements, data security, reliability, systems integration, language capabilities etc., Nina is PCI compliant, with enterprise-grade SLAs; integrates easily with a wide range of third-party systems, including CRM and knowledge management solutions; and supports close to 20 unique languages in over 25 regions worldwide.

Where Is Nina used?

In terms of the kinds of situations in which virtual assistants can be used, there are three increasingly sophisticated categories where Nina can add value:

- General inquiries that do not rely on an enterprise's backend data or require user authentication, but which typically take undue time and effort for users to find on a website – such as contact information, directions to offices, operating hours, opening times etc. – resulting in customers being forced to escalate their query by calling into the contact center.
- Searches which, for optimal performance, can involve backend data, but where the user remains anonymous such as hotel booking information (rates, availability), merchandise inventory, pricing checks, etc.
- Requests that need both backend data and authentication for highly personalized interactions – such as banking transactions, access to health records, etc.

Which Channel to Start with?

For many consumers, the Web is their preferred first place to inquire – increasing call deflection improving ROI as the Web is a low-cost channel. Because Nina delivers significant benefits without backend integration, many enterprises' first step is therefore to add the virtual assistant to their website or mobile app to enhance their existing Web presence.

• You could, for instance, deploy Nina as anything from a simple text-based chatbot to an omnipresent avatar that sits on multiple highly trafficked pages on your website or mobile app, and acts as a first point of contact for your customers – answering their queries, or helping them instantly find the information they need, rather than having to search for an FAQ or other relevant pages.

- The targeting engine enables Nina to be available proactively to the consumer, based on a variety of parameters, including time on page, browsing history, and specific business conditions, etc.
- This can be particularly helpful if your website has long or complex FAQs that visitors find difficult or time-consuming to navigate, or if you want to keep the user in a flow, such as guiding them to a checkout while they search for answers to questions that might otherwise cause them to drop out.
- You could also integrate Nina with your contact center to offer live chat, so that if a customer requests help from a live chat agent (or the virtual assistant is unable to confidently answer their query), details of Nina's conversation with the customer are automatically passed to the appropriate agent to assist with resolving the issue.
- And you could extend Nina's scope by making the virtual assistant accessible to internal employees – for example, to provide a source of company-related information such as questions about training, where to go for particular resources, etc.

Integrating with CRM

To make more of Nina's intelligence, the virtual assistant needs access to a broader range of data, so the next step will often be to integrate it with backend systems such as contact management, CRM or a marketing automation solution like Salesforce.com. This is so that when a customer logs in to your website or mobile app, Nina will be able to access information about them and provide a more interactive, personalized or proactive level of service. For example:

- An airline or travel company's virtual assistant could be aware that a customer contacting it has a flight booked within the next few days and is likely to want to check that their flight is on time or has not been cancelled. In this case the virtual assistant could begin the conversation by asking if they want to check their flight details.
- For a car rental company, if someone logs in to their account and the virtual assistant knows they have a car that is shortly due to be returned, it could ask if they'd like details of how and where to return it or if they want to extend their rental a situation where integration with financial systems will also be beneficial.

Nina also integrates with existing authentication and verification systems to ensure the person is who they say they are without ever leaving the conversation with the virtual assistant.

ERP, Financial and Other Data

The third major area for backend integration is with ERP (enterprise resource planning), financial and/or other information systems.

- Integrating with ERP enables customers either anonymously or via their account to check information such as product pricing and availability, discounts, delivery schedules and more.
- Integrating with financial systems aids in order processing, sales enablement, up-selling and increasing average basket size. It can also increase cart completion by helping customers navigate difficult parts of the website or fill out complex order forms.

• The customer experience can also be enhanced by location-based data. For example, if a telecom service provider's virtual assistant knows there is a service disruption in the area in which a customer is located, it can proactively inform them about progress in fixing the issue and when the service will be back up and running.

Delivering a Consistent Experience

In addition to supporting these very different types of applications, Nina can deliver a consistent customer experience across multiple channels, without the need to create or code multiple applications – reducing total cost of ownership.

Automated webchat: Nina can help ensure customers quickly and easily resolve issues on the channel they turn to first by providing a concierge-like experience without the need for a site redesign.

Mobile apps: Incorporating Nina into an existing native app improves discoverability, increases self-service resolution rates, encourages repeated use, and brings your app to life.

Text messaging: Nina creates a natural two-way automated dialogue that lets you engage customers through proactive reminders or responses to messages sent to your text numbers.

Messaging apps: Plugging Nina into emerging channels like Facebook Messenger allows users to connect with your brand in a simple and conversational way on their channel of choice.

Smart home speakers: Integrating Nina into devices like the Amazon Echo or Google Home allows your customers to interact with you hands-free by using their voice.

The Nuance Digital Engagement Platform enables a design-once, deploy anywhere approach whereby companies can easily and cost-effectively extend their investment to multiple channels and continuously optimize automated and human-assisted customer experiences, thereby reducing costly one-off channel implementations and multiple backend integrations.

Deployment

Nina helps clients quickly achieve goals through human-assisted AI and machine learning. Each Nina deployment is overseen by Nuance's Professional Services team, who are experts in creating the dialogue, designing the conversation, and verifying the questions asked by consumers. This enables Nina to be implemented very quickly – with initial deployment in as little as a few weeks.

- Nina's 'out-of-the-box' social dialog, industry specific content and language skills enable it to excel in back and forth conversations, basically natural interactions that allow customers to better articulate what they're looking for or trying to achieve, just as if they were talking to real human being.
- Nina leverages existing call and chat transcripts and absorbs this conversation data to create a first version of a branded virtual assistant. Machine learning algorithms cluster this data and ensure that your virtual assistant knows how to handle these questions.
- In order to assist the virtual assistant during its first conversations, it can be deployed with a direct connection to its human colleagues. That allows Nina to ask for help if a question cannot be mapped to an answer yet.

Depending on the specific inquiry, the human can either select the correct answer and Nina continues the conversation or the human takes over and seamlessly moves the user from an automated to a human assisted conversation.

Once Nina has been deployed it learns from every interaction, no matter if automated or human assisted and either applies the new knowledge to the existing "brain" or incorporates it to expand the topics it can talk about. This feedback loop is important for the continuous learning process to ensure Nina is always on top of every conversation.

Analytics

Nina includes analytics capabilities providing a comprehensive view of what's happening within the customer journey and how well engagements are being handled. These range from high level insights (how many things were understood, how many sessions ended with an answer, how many users dropped out of a conversation) and detailed analysis of the overall performance (e.g. where Nina did not understand something, what training is needed to address this) to logs of individual conversations. This can be vital in ensuring compliance in industries such as finance and healthcare, as well as for continuously improving Nina's performance.

Besides engagement activities, Nina's reporting can drill down to specific customer acquisition and customer care KPIs, giving enterprises the opportunity to estimate the influence of their virtual assistant into their everyday business outcomes. The central data repository stores current as well as historical data for creating default and custom reports and this data is collected and analyzed to construct, refine and optimize dialogue and website behavior.

What Happens in a Typical Deployment?

Although every organization is different and there is no 'off the shelf' version of Nina, the Professional Services team applies a common collaborative process to every deployment of the virtual assistant.

Your goals: The starting point is agreeing what you want to achieve. What are your current concerns and how can we help you address them? Do you want to improve sales, streamline customer service or offer more options for your customer to engage with you?

Your use case: To achieve your goals, the team will work with you to define the use cases, processes and conversational flows based on your individual challenges, for example:

- If you want to provide an intelligent interface to your FAQs, this could be as simple as defining answers to a standard set of questions related to a fairly static set of content.
- If the aim is to deflect contact center calls, the exercise could look more broadly at why people are calling your contact center and how Nina can help them achieve the same result without leaving your Website for example by providing an easier.

Your avatar: In parallel with this the Professional Services team will discuss with you and your branding team what your virtual assistant will look like. Will you have an avatar, will it be embedded into or float over various pages, what tone of voice should it have, way of answering their questions, or leading them through clear step-by-step processes.

Integrations: As well as agreeing your virtual assistant's content, branding and persona, the Professional Services team will assist with any technical integration. For example, if you

wanted to create transactional use cases such as enabling customers to pay a bill or check their account balance, the team will work with you to define and build APIs enabling secure access to and control over the information flows required.

Once your use cases and content have been defined, the team will use a natural language model to import for example huge quantities of chat transcripts or spreadsheets of the many things customers might say; group common topics, issues and phrases into customer intents; test that these accurately reflect what's happening in your customer interactions; tailor the responses you want your virtual assistant to make; and then automatically generate your initial language model.

In addition to this language model, the process aspects of how Nina behaves – how it responds if it doesn't understand a customer, how it asks them to rephrase their query, and what it does next, such as offering live chat or a contact phone number – are fully customizable. And Nina can automatically switch into different modes, depending on how a customer is behaving – for example, if they want to be contacted; they're expressing frustration, criticism, dissatisfaction, profanity etc.; or the question they're asking is beyond the virtual assistant's scope.

Pre-production testing and optimization: Depending on the complexity of your deployment, in as little as 4-6 weeks you could have a working version of your virtual assistant, which can then either be used for an iterative process of pre- production and testing or already deployed with a human coach standing by to assist Nina during first conversations.

Go live! At the end of this optimization you will be at a point where customers can actually communicate with your virtual assistant, and it can go live on your website. The Professional Services team will then continue to tune Nina for approx. another month so it learns any additional phrases your customers might be using.

Continuous optimization: Throughout the life of your virtual assistant, the Professional Services team will continue to provide guidance and support, leveraging best practices from across the Nina installed base to help it continually improve and evolve – through regular conversation reviews, reports, and assistance with adding new content (e.g. related to organizational or process changes, new product launches, etc.).

Results

Right now, Nina provides intelligent support and assistance to the customers of leading global enterprises in industries including airlines, automotive, education, entertainment, financial services, healthcare, manufacturing, pharmaceuticals, technology, telecom and travel. Across all of these industries, Nina is typically achieving First Contact Resolution (FCR) rates of 75-85% (the same rates associated with live human agents), and deflection rates of 40-70%.

Coca-Cola, Jetstar, Swedbank, Australian Tax Office and Windstream are among the many companies benefiting from Nina's advanced capabilities. At Jetstar, for example, Nina averaged over 250,000 conversations per month, freeing up agents to assist with atypical requests, and achieved 85% FCR, plus a 20% reduction in calls per 1,000 passengers. At the Australian Tax Office, meanwhile, Alex engaged in 2M+ conversations within the first 18 months, achieved 88% FCR, which resulted in \$9.7M in client red tape reduction savings yearly.

Nuance Communications, Inc.

Nuance was founded in 1994 as a spin-off of SRI International's Speech Technology and Research (STAR) Laboratory to commercialize the speaker-independent speech recognition technology developed for the US government at SRI. Nuance deployed their first commercial large-scale speech application in 1996. Their initial route to market was through call center automation. Call centers had just centralized the branch-office telephone handling function throughout many large companies. The highest cost of running call centers is the cost of staff. Early projects were completely developed by Nuance to prove the commercial practicality and benefits.

Today Nuance Enterprise, is reinventing the relationship between enterprises and consumers through customer engagement solutions powered by artificial intelligence. Nuance aims to be the market leading provider of intelligent self- and assisted- service solutions delivered to large enterprises around the world. These solutions are differentiated by speech, voice biometrics, virtual assistant, web chat and cognitive technologies; enabling cross-channel customer service for IVR, mobile and web, Inbound and Outbound; and magnified by the design and development skill of a global professional services team. Nuance serves Fortune 2500 companies across the globe with a mix of direct and channel partner selling models.

Kasisto: Virtual Assistant¹¹

Siri's descendants will soon improve customer service at a wide variety of companies. SRI International (best known for inventing and selling Siri to Apple in 2010), is now creating virtual assistants that can help customers perform complex tasks in banking, shopping, and business.

While assistants like Siri know a little about a lot of things, virtual specialists have a narrow main focus, but their knowledge in that subject is very deep, thanks to natural language processing and artificial reasoning capabilities.

If you say to Siri, 'Transfer \$200 to checking,' Siri will look up transfer on the web, and probably point you to Wikipedia. But when you walk into a bank, you expect the person behind the counter to know a lot about banking and help you with your banking needs. That's the vision for the assistants SRI is starting to put together.

SRI has built a platform that makes it easy to build these specialized assistants in different industries. They could be used in any field that requires an interaction, including for a retail purchase, a healthcare consultancy, or an insurance query. These assistant bots could live in a company's app or website, or in a physical space, like a kiosk at a store. The goal is to improve interactions and the customer experience.

When you try to do anything complicated in real life, you're going to be involved in a conversation of some kind. When SRI designs these computer systems, not only do they need to know about banking, but they also need to know how to have a conversation, where new intentions are introduced into a conversation, without forgetting that old intentions are not satisfied yet.

For example, a conversation with a bank teller or a specialized banking assistant bot might open with the customer saying, "I want to transfer \$200 to my checking account." The bot would have to ask from which account to extract the money and be able to answer other questions such as "How much do I have in savings?" while still remembering the original request. This requires deeper knowledge, and deeper conversations.

¹¹ https://kasisto.com/kai-banking/on-mobile/

Kasisto understands how consumers interact with banking systems. The most important thing to learn is that virtual assistants are not apps – what people do in normal banking apps is not the same as the way they do banking in conversational systems.

Mobile banking tends to be transactional – a person might log in to check their balance, or transfer money. With the smart bots, people tend to do things they couldn't do on a regular banking app, using the power of human language to ask questions such as "How much did I spend on Uber last month?" or "What was my largest restaurant transaction this year?"

The biggest obstacle for companies building a virtual assistant is the amount of work and expertise it takes. SRI is building a piece of software that already has a significant part of the solution. Things like speech recognition, natural language understanding, and core reasoning capabilities are all built into the platform.

Real Tasks

Kasisto also knows a lot of detail about banking, and is able to help users perform real banking tasks through conversations such as this one:

Consumer: I would like to make a payment on my credit card from my checking account.

- Kasisto: The minimum payment amount on your credit card account (Gold Plus Credit Card *2234) is \$159.73. Is this the amount you want to transfer?
- Consumer: No, I would like to pay \$2,000.
- Kasisto: I am sorry you have only \$1,544.78 in your checking account (Checking *9072). That's not enough to complete this transfer. Would you be interested in transferring \$2,000 from savings account (Savings *9076) to your credit card (Gold Plus Credit Card *2234)?

Consumer: No, please pay \$1,000 from checking today.

Kasisto: I can do that. To confirm, you would like to transfer \$1,000 from checking account (Checking *9072) to credit card (Gold Plus Credit Card *2234). Is that correct?

Consumer: Yes, thank you.

This interaction, and almost all interactions within banking services (and retail, healthcare, etc. services) have an element of discovery: users refine their intents and learn more about the service through conversation. The virtual specialist must combine conversation with reasoning based on deep knowledge in order to fulfill the user's intent.

For example, Kasisto needs to know that credit card bills have minimum payments and that when the consumer says "pay \$2000," he or she is referring to the credit card bill (because bills are things that are paid and the only bill in the conversation is the credit card bill). Finally, in a real conversation both parties are proactive. As a good virtual specialist, Kasisto proactively warns the consumer about insufficient funds and alternative payment options.

Proactivity is in fact a key characteristic of a specialist, indeed any assistant. We expect assistants to anticipate our needs, help us discover relevant new things, and work in the background on our behalf. Automated proactivity is a tricky business: the assistant needs to understand the user's context and intent and make only useful suggestions. Much of human behavior is routine, creating predictable context and intent (most people leave the same place at about the same time to go to work).

But we don't need much proactive help with this part of our life. We want to be told about things that will disrupt our routine (unusual traffic situation, first meeting canceled, etc.), but the proactive help required in these situations is itself pretty routine and is becoming commoditized. Some assistants also proactively tell us "interesting" things. These can be useful (e.g., your boss's birthday is tomorrow), but are often distracting, and are too often simply advertisements.

It is during non-routine behavior – when we are looking for something new, doing something unfamiliar, trying to fix a problem – that we most need proactive assistance. This is the realm of the specialist. Deep knowledge enables specialists to give much more targeted and useful proactive assistance. As we have seen, detailed knowledge of the consumer's account and bank rules enables Kasisto to provide useful proactive guidance.

A virtual healthcare specialist could learn from the content and style of a user's conversation that a proactive suggestion about diet or medication is warranted. A virtual retail specialist can tell a consumer's shopping expertise from their questions and vocabulary, enabling it to make proactive suggestions that the user will understand and appreciate.

This is only the beginning: much of what people do in the real world involves conversational interaction with specialists ranging from waiters to bank clerks to medical professionals. The rapid worldwide adoption of mobile devices requires us to move beyond virtual personal assistants to create the virtual specialists that will enable consumers to really get things done through their mobile devices.

Crossing the "Valley of Death": Cybersecurity Research into Practice

The challenges of transitioning technology from research to real-world deployment occur in all areas of technical research, and are generally not unique to cybersecurity.¹² However, at this time, it is extremely important to significantly improve the success rate of technology transition in the cybersecurity field. The cybersecurity problem is bigger than ever, with government and industry being victims of severe attacks, including successful attacks against companies that specialize in security technology. For the past several years, we have seen rampant theft of sensitive information and intellectual property. We are also starting to see destructive attacks, some even targeting critical infrastructures.

New and innovative solutions are desperately needed to get the problem under control, and those solutions must be widely deployed in operational settings to make a difference. Two key actions are needed, on a national level: 1) We need to increase R&D funding levels, and 2) we need to get much better at taking the best results of R&D all the way to deployable solutions. If we were to fail to accomplish both of these actions, the nation would be set up for a disaster some years from now, when it would not have security solutions developed to match the challenges of the rapidly evolving world of information technology. It is therefore in the best interest of our entire society to make sure that technologies are transitioned from the research into the hands of users.

There are many promising technologies that are currently undergoing research and development, and while that is absolutely necessary, it is not sufficient. We cannot afford to have technologies be put on a shelf because the funded projects ended and the researchers moved on to new problems that were yet unsolved. When a solution to a problem is being developed, we must

¹² We use the term technology transition to broadly describe all efforts to ensure that technologies developed in research settings will eventually be deployed and used operationally. We do not make the distinction between technology transition and technology transfer that is sometimes used in the DoD community.

also ensure that the solution meets the needs and requirements of users and it is made available for deployment via channels that are acceptable to the users. To achieve widespread operational deployment and use, solutions can for example be made available directly to users as commercial products or as open source, or indirectly by providers or operators of critical infrastructure.

There are many reasons why technology transition does not happen easily. It is usually not an issue of researchers being unwilling to support transition – most researchers want to see their work have an impact – but good intentions are unfortunately not sufficient. There are differences in the personality types and skills that are suitable for computer science and engineering research versus those that are suitable for business, customer interaction, and entrepreneurship. There are counterexamples of successful individuals who possess all those skills, but it is a rare phenomenon. Incentives to encourage technology transition may also be lacking.

A researcher whose success is measured in the number of peer reviewed publications and academic honours may not be motivated to spend a lot of time and energy on technology transition. Depending on the research organization, there may or may not exist direct financial incentives for researchers to pursue commercialization of their results, such as royalties or shares of a startup company. Even when such financial incentives exist, they may not serve as sufficient motivation due to the personalities and organizational culture often found in research environments. Furthermore, if research project funding does not explicitly include technology transition efforts, researchers may not be able to perform the work associated with transition unless they can find another way to fund it.

A metaphor that is often used to illustrate the challenging gap that exists between research on one hand, and operational technology use on the other, is "The Valley of Death" – see Figure V.13. The first use of The Valley of Death metaphor to describe the gap that must be bridged in a successful technology transition effort is attributed to Congressman Vern Ehlers, and variations of this theme have since been used.



Figure V.13. The Valley of Death Between Research and Industry

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Numerous studies have been performed and reports written on the difficulties and challenges of technology transition in Government funded R&D and approaches to overcoming those challenges. A 2004 National Academy of Sciences report noted inefficiencies and long delays in the transition of new technologies due to complexities in the research, development, and transition processes and differences in the goals, timeframes,

and funding levels of the different players in the process (researchers, industry and operational users)¹³.

The report identified active collaboration among researchers, industry, and operational users during all phases of technology transition as a key goal for success. Similarly, a 2007 Department of Defense report to Congress on technology transition, cited evidence of a chasm between the Science and Technology (S&T) and acquisition communities, i.e., the "valley of death", which could be bridged only through cooperative efforts and investments by both communities.

To overcome these challenges and improve the technology transition track record in the cybersecurity R&D community, we need to share experiences, working models, and best practices for technology transition. SRI has developed a research and development (R&D) execution model to significantly increase the success rate of technology transition, based on experience from cybersecurity programs in R&D funding agencies.

While the model was developed by the cybersecurity R&D program at the United States Department of Homeland Security Science and Technology Directorate (DHS S&T), it is generally applicable to other R&D organizations. In fact, other R&D funding agencies already practice portions of the model.

Despite the challenges, the DHS S&T cybersecurity R&D program has successfully transitioned a number of R&D technologies from research into widespread deployment and use where they are having a real impact on operational cybersecurity.

IronKey received R&D funding to develop a secure universal serial bus (USB) device and has grown from a small start-up into a thriving company supporting widespread use of their product. Endeavor Systems received Small Business Innovative Research (SBIR) funding to develop a botnet detection and mitigation tool that led to their acquisition by McAfee.

The Open Information Security Foundation (OISF) received funding to develop Suricata, an open source intrusion detection and protection system, creating a strong development community that continues to develop the product to meet unmet IDS/IPS needs. To illustrate the effectiveness of the R&D execution model, we will further describe these examples of successful technology transition from the DHS S&T cybersecurity program. Such examples serve to show that given the right model, cybersecurity R&D programs can transition research results into operational use where they can have an impact on cybersecurity.

Key Elements of Transition Success

Before presenting the model, we describe some key elements that we find to be vital to repeatable, successful technology transition, based on our experience and observations:

Pervasive emphasis – by design, technology transition should be an integral part in all aspects of an R&D program. In any program plan, call for proposals, review process, funding vehicles, Principal Investigator (PI) meetings, site visits/reviews, reports, and all other program activities and metrics, technology transition should constitute a key requirement and evaluation criterion.

¹³ Accelerating technology transition and bridging the valley of death for materials and processes in defense systems, National Academy Of Sciences, 2004. (http://books.nap.edu/catalog.php?record_id=11108)

Early involvement-technology transition should be designed into the program from its first inception. This includes a program plan that is based on a firm understanding of customer needs and requirements.

Active engagement – technology transition is an active sport, where success requires significant effort throughout the entire process. Researchers and program managers must engage the customers (the identified end-users of the technology) and keep them engaged before, during, and after the execution of the research. This includes identifying and selecting specific customers that are ready and able to be involved in the entire process.

Tangible support – the agency that funds the research should also provide its performers with support that is dedicated to technology transition. This includes providing funding for technology transition activities, providing and requiring specialized innovation training for researchers, organizing events such as technology showcases and matchmaking, and providing introductions and connections between researchers and potential technology customers.

It should be noted that there is not just one single path that can lead to successful technology transition. On the contrary, multiple alternative paths exist and some are better suited than others for certain R&D organizations and customers.

Large companies gain access to new technologies produced by their own internal R&D teams, or by licensing technology from outside labs or small companies, or by acquiring a small business. The large company would then typically commercialize the technology through their own product portfolio and sales channels.

A small business such as a startup company can get R&D funding from government agencies, for example via the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs – funding that can boost technology development and supplement funds from other investors. To ultimately be successful, a startup company may require external funding, such as angel funding or venture capital, at some stage of its growth. Experienced venture capitalists are known to provide important support and guidance for technology transition, in addition to providing the funding itself. Licensing and acquisition are avenues that can feed technologies from small businesses into the sales and support apparatus of a large company.

For academia and research labs, licensing technology directly to an established company can be an effective transition path, while more adventurous and driven researchers who have the right kind of support from their institution can take the path of founding a startup company. While some institutions have offices and programs dedicated to support licensing and ventures, many show remarkably little interest in supporting technology transition and any success is typically the result of extremely dedicated efforts by the inventors themselves. For all R&D sources of new technology, open source is an alternative to traditional transition channels. A number of government programs encourage or require technology to be released under open source licensing, as part of the R&D activities. Open source availability is well documented as a powerful and effective means to bring important capabilities into adoption, use, and support by larger communities.

There are many interrelated factors affecting technology transition, including time and schedule, budgets, customer or end-user participation, demonstrations, testing and evaluation, and product partnerships. Given these factors, and because one transition path can be a better fit than another, funding agencies may not want to require a specific transition path (such as

open source). Instead, the funding agency should work with each of its performers to help them identify the best transition path depending on the specifics of the R&D organization, the technology, and the customer.

A Proven R&D Model

The R&D execution model is a template for how the key elements of transition success above can be implemented as an integral part of a cybersecurity R&D program. The model is shown in Figure V.14 and is affectionately known as the "Circle of Life". It is comprised of a continuous cycle of requirements gathering, pre-R&D, R&D, and post-R&D activities oriented towards technology transition. The cycle begins with collecting prioritized requirements from customers and critical infrastructure owners and operators. Pre-R&D activities include the development of research agendas to help align research programs with community needs and solicitations that result in research programs focused on satisfying those needs.

R&D execution involves program support activities that ensure researchers, program managers, and customers continue to work together to develop innovative technologies that can be transition for operational use. It also involves testing and evaluating technologies with realistic data as an integral part of the research. Post-R&D activities involve technology transition and deployment activities, including technology assessments and evaluations, experiments and pilots, and outreach.



Figure V.14. Cybersecurity R&D Execution Model for Technology Transition

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Assessments and evaluations ensure that technologies are vetted prior to operational deployment. Experiments and pilot deployments allow technologies to be tested and evaluated with real users in real operational environments. Finally, researchers must also conduct outreach to promote their technologies and attract transition partners. In short, the model includes the full spectrum of necessary activities – research, development, test, evaluation, and transition (RDTE&T) – needed to develop completed "research products" that are tested in the hands of operational end-users and potentially result in widespread deployment and use. We will describe all of these activities in further detail in the following sections.

Customer requirements

The model starts with collecting prioritized requirements from customers and critical infrastructure owners and operators. It is essential for researchers and government program managers to know and work with the customers or ultimate users of the technologies that will result from research. Direct interaction with operational users enables researchers to identify and articulate critical requirements and develop solutions that will solve operation challenges and problems, and fit into operational systems, processes, and procedures.

Such interaction is not easy; customers and users are often busy addressing their primary job or mission, with limited time to interact with researchers. Researchers must push their customers to think beyond incremental changes to their existing tools and technology and consider radically new technologies and tools that can solve the problems and needs of the future. Operational needs and requirements must be expressed as research problems that can be understood by researchers. By identifying future needs today, researchers can begin to develop solutions for potential transition tomorrow. If current needs had been expressed yesterday as research challenges, then there would be technologies available today to satisfy those needs.

Collaborative Research Agendas

Having clearly identified and articulated research challenges and requirements helps focus R&D on developing solutions to current and relevant problems. It is important to both contribute to and draw from the collaborative research agendas to ensure alignment of research with overall community priorities. Coordinated US Government cybersecurity R&D efforts and groups include the White House Comprehensive National Cybersecurity Initiative (CNCI), Networking and Information Technology R&D (NITRD), Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), and the Special Cyber Operations Research and Engineering (SCORE).

These groups and others have developed a number of national documents that define research agendas and priorities for cybersecurity research. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* [6] defines a set of interrelated priorities for U.S. government agencies that conduct or sponsor cybersecurity R&D and organizations that perform the R&D. An inter-agency group comprised of members from DARPA, DHS S&T, DoD, DoE, IARPA, NIST, NASA, NSA, NSF, and others, working in coordination with the academic and industry research community, developed the plan. It describes and prioritizes end-states and capabilities that must be achieved to secure cyberspace and hence provides strategic guidance for R&D efforts.

Similarly, DHS S&T's document, *A Roadmap for Cybersecurity Research* [7], provides detailed research and development agendas and defines 11 hard problem areas in cybersecurity, for use by government agencies and the research community. Groups in various critical infrastructure sectors have also defined their own sector-specific research agendas and plans, such as banking and finance [8] and energy [9].

Pre-R&D Solicitations

The development of solicitations, such as a Broad Agency Announcement (BAA), used to request research proposals and ultimately fund research programs and activities, are another critical aspect of pre-R&D activities. The solicitations must clearly articulate the research

goals, objectives, and requirements in order to ensure that the proposed research is properly targeted towards the desired research problems and needs.

The solicitation must identify and provide detailed descriptions of the technical topics areas (e.g., software assurance, enterprise-level security metrics, usable security) so that the researchers can propose solutions that address the right technology needs. The technical descriptions should include necessary background information and references, the problem to be solved, the types of solutions that are potentially applicable, illustrative examples, and performance metrics. The technical topics should be derived from customer requirements and align with an organization's strategic plans as well as external plans, such as those resulting from the collaborative efforts of the CNCI.

Technology transition must be an integral component of a solicitation. Researchers must be compelled to consider technology transition before, during, and after their research and include technology transition as an integral component of the proposed research activities. To accomplish this, they should identify the maturity level of their proposed solution and the amount of time, effort, and funding needed to complete the solution and transition it into widespread use. Relatively mature technologies may only require funding for a short timeframe to conduct technology demonstration in an operational environment.

Prototype technologies, which are less mature, need a longer timeframe with a development phase as well as the demonstration phase. And new technologies, which are even less mature, need an even longer timeframe with applied research, development, and optionally demonstration phases. A structure such as this supports immediate transition wherever possible, and starts to create transition paths for newer, less mature capabilities by having the researcher consider and commit to ultimate transition from the outset of the proposed research.

These levels of maturity are a simplified form of the Technology Readiness Levels (TRLs), initially developed by National Aeronautics and Space Administration (NASA) and widely used by the Department of Defense (DoD). The TRLs are a series of nine increasing levels or measures of maturity of a technology to be incorporated into a system or sub-system. The TRLs provide much greater granularity and are oriented towards traditional systems and software engineering, making them more suitable for large systems integration efforts. We believe the three simple levels are better suited for academics, small startups, etc. who are developing research prototypes and proof-of-concepts.

For all three maturity levels, researchers should be compelled to provide a commercialization plan or other plans for getting the technology into established transition paths, including commercial partnerships or the open source community. The intent is to force the researchers, as part of their technical plan development, to consider the ultimate commercialization of their research results, including considerations such as what is the expected user base, how the technology will be used, and how it will transition in to broad use. Of key importance are the identification of technology transition paths that are appropriate for the type and maturity of the technology involved, and any additional factors that might increase the likelihood of it being commercialized.

R&D Execution

The activities of the execution phase of an R&D program are critical to developing technologies that meet important customer needs. The commitment to technology transition that began in the solicitation (pre-R&D) phase is continued in the execution phase. The researchers, as well as project management staff, are reminded of the need to make technology transition a critical part of the research effort. Support and resources are also provided to help increase the chances of transition success.

R&D stakeholders (customers or users who provided the initial prioritized R&D requirements and potential transition partners) are engaged and invited to participate throughout the execution phase. Stakeholder feedback is regularly sought through demonstration of developed prototypes. The important elements of the R&D model and the important role of the stakeholders are regularly emphasized, not only to keep stakeholders engaged, but also to remind the PIs that the customer need (and eventual satisfaction) is what is driving the R&D program, not the innovative technologies themselves.

Bringing many R&D performers together as part of a research project portfolio introduces complexity in managing both the individual projects as well as the portfolio. Providing all the researchers, as well as the program managers (PMs), with innovation training gives them a common framework to discuss and define customer requirements, conduct research, and describe project success is one way to reduce the communication complexity of leading multiple projects towards successful transition. One such framework, the Five Disciplines of Innovation (5DOI) [11], is practiced and advocated by SRI International. Briefly stated, the five disciplines are:

- Important Customer Needs (I) begin with a meaningful problem
- Value Creation (V) have a common language to discuss and create value
- Innovation Champions (C) appoint someone who is passionate about the project and its success
- Innovation Teams (T) ensure collaboration within and across teams
- Organizational Alignment (A) manage to achieve innovation success

As shown in Figure V.15, the elements are all needed to achieve market success.

Figure V.15. SRI's 5 Disciplines of Innovation. All must be present for success



Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

As part of the cybersecurity R&D program at DHS S&T, lead researchers and PMs are given innovation training in which they learn the 5DOI, refine their presentation skills to help focus their value proposition, develop habits of collaboration, and become accustomed to the focus on customer needs and successful transition.

Throughout the R&D process, for both individual projects and the project portfolio, technology demonstrations, road mapping activities, and technology workshops are held to demonstrate continued value and to elicit feedback from customers, users, researchers, and other stakeholders. PI meetings, traditionally a rote exercise of reciting plans and milestones, are used as interactive forums where researchers, managers, and customers can provide valuable feedback to each other and find areas of mutual interest or collaboration (a "watering hole" in the 5DOI lexicon).

It is critical that new R&D technologies undergo test and evaluation (T&E) as an integral part of the research, starting from the beginning and continuing throughout the effort. Making research infrastructure, such as test facilities and realistic datasets directly available to researchers make it easier and more likely that they will test and evaluate their technologies with respect to system performance goals. Performers may use the facilities of the Cyber Defense Technology Experimental Research (DETER) testbed or they may use other facilities as appropriate. The DETER testbed provides the necessary infrastructure – networks, tools, and supporting processes – to foster national-scale experimentation on emerging security research and advanced development technologies.

Similarly, performers are free to provide their own datasets, or they can use those available through the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PRE-DICT). PREDICT was developed in response to the ongoing need for datasets and the problem for the networking and information security research communities. The goal of PREDICT is to create a national R&D resource to bridge the gap between the producers of security-relevant network operations data and technology researchers, developers, and evaluators. Using test facilities such as DETER and realistic test data from sources like PREDICT enables researchers, developers, and evaluators to accelerate the research, design, production, and evaluation of next-generation, cybersecurity solutions that can lead to commercial products.

Post-R&D Activities

Post-R&D activities are for the most part directly focused on transitioning research results to customers and potential users. In this phase, researchers must broaden the scope of their transition activities and expose their technology and tools to a wider audience. Post-R&D transition activities include technology assessments and evaluations, experiments and pilots, and outreach to potential investors and users.

Assessments and evaluations ensure that new cybersecurity technologies are vetted prior to operational deployment within potential user environments. They are conducted through technical assessment, modeling, vulnerability and risk analysis and red team evaluations and operational assessments. Such efforts impact and influence the entire cybersecurity community, both within the Federal government and in the private sector, in identifying and assessing cyberthreats and vulnerabilities and assisting in the acquisition, evaluation and deployment of cybersecurity technologies.

Operational users need experimental deployment opportunities to investigate operational capabilities of the new technologies. Experiments and pilot deployments allow for R&D technologies to be tested and evaluated with real users in real operational environments and provide feedback for researchers and vendors. The feedback also allows operational users to validate and refine their requirements and ultimately make their systems and infrastructure more secure.

As part of their post-R&D activities, researchers must also conduct outreach to increase awareness of emerging commercial technologies and gain insight of cybersecurity needs and requirements of investors, vendors, and users looking to engage these potential new suppliers. Researchers may attract systems integrators or large companies to whom they can sell or license their technologies. Researchers may also attract investors who are willing to provide funding needed to create spin-offs or small business start-ups that can commercialize their technology in hopes of eventually growing into the marketplace or being acquired by a larger company. It is important to identify potential users or marketplaces to help justify investment and creation of commercial products.

There are many ways to reach out to potential investors, vendors, or users. In addition to individual efforts by PIs and government program managers to promote their R&D technologies, they can also participate in collective efforts such as community events and technology showcases. TheDHSS&T cybersecurity program has initiated a number of such outreach activities. Three examples include the Infosec Technology Transition Council (ITTC), the Security Innovation Network (SINET), and the System Integrator Forum.

The ITTC is a working forum, created by DHS S&T and SRI International, where experts and leaders from government, private, financial, IT, venture capital, academic, and science sectors come together several times each year in the San Francisco Bay Area to address a variety of problems related to cybersecurity technology.

The primary objective of ITTC is to identify proactive IT security solutions and to assist in the acceleration of their development and deployment into the market place. Seasoned professionals in IT security and law enforcement, together with representatives from academia and science, strategically align themselves with subject-matter experts and organizations to pursue this objective. Recent meetings have included talks by current and former government officials, FBI, Secret Service, legal experts, critical infrastructure providers, and members of the research and development communities.

SINET is a non-profit organization, supported in part with DHS S&T funding, that fosters collaboration and provides a number of opportunities to engage the community. SINET brings together members of the Federal Government, IT and security providers, systems integration, venture capital, investment banking, and the academic and science communities.

The SINET IT Security Entrepreneurs Forum (ITSEF) and SINET Showcase link technology creators, developers, investors and users in key technology markets around the country. ITSEF is held at Stanford University in the heart of Silicon Valley. SINET Showcases are held in Washington, DC and other major cities around the country to provide a venue for innovative security companies to present technologies that meet industry and government needs.

The DHS S&T System Integrator Forum is an example of an outreach event, held in 2007 and 2008, which brought together system integrators and government sponsors of information systems projects and showcased several new cybersecurity solutions funded by DHS S&T. The forum introduced high-quality, top-performing cybersecurity technology development projects funded under DHS BAA or SBIR programs to large integrators of technology who serve the federal government and private industry. Participants were selected for the maturity of their solution, relevance to government needs, the commercial viability of their approach, and their business leadership.

Successful Use of the Model

Technology transition from research into current, emerging, and future systems is clearly and explicitly stated as an integral part of the DHS S&T cybersecurity R&D program mission and goals. To accomplish this mission and achieve these goals, the program developed and fully employs the R&DExecution Model described above. At the core of the model is the Cyber Security R&DCenter (CSRDC), which brings together and facilitates all the elements of the model.

The CSRDC plans, coordinates, manages, and conducts activities to secure cyberspace. CSRDC works with research organizations, critical infrastructure operators and developers, and others. Its activities are all focused on successful technology transition and include the development of the cybersecurity research roadmap, research program management, testbeds, experimentation and exercise development, and coordinating various government-industry collaborations.

By applying the R&D Execution Model, in which technology transition is built-in as an integral component of the RDTE&T lifecycle, the DHS S&T cybersecurity R&D program has successfully transitioned technologies from funded projects (including SBIRs) into the commercial market place through spin-offs, acquisitions, and commercial products, including open source software. Table 1 lists several examples of such technology transition successes. These successes serve to show that the R&D Executions Model is not just an abstract model; it's employed by DHS S&T and it works to drive successful cybersecurity technology transitions.

Below are brief recommendations for the actions of researchers and research managers:

Table V.4. What to do and not do in R&D Technology Transition

Researchers DO

Interact with the eventual users of your technology and gain understanding of their needs and requirements.

Learn how to develop a value proposition that articulates your understanding of the need your solution meets, and quantitatively describes benefits users gain deploying your solution.

Use the transition support resources available from your institution and your funding agency.

Researchers DO NOT

Think that your solution will "sell itself". Even the best products need marketing.

Describe your solution only in terms of the technical approach.

Give up. There are many challenges to overcome in technology transition, and it often takes many failed attempts before success is reached.

Program Managers DO

Interact with the eventual users of the technologies to be developed in your program and gain a thorough understanding of their needs and requirements before you solicit research proposals.

Make technology transition a key requirement and evaluation criterion in all aspects of your program.

Guide and support your performers in their technology transition efforts, by providing funding and training, organizing events, providing introductions and connections to potential technology costumers, and helping each of your performers identify the best transition path for their organization, technology, and customer.

Program Managers DO NOT

Think that technology transition is the responsibility of someone else. You are in a unique position to facilitate and enable successful transition for technologies developed in your program.

Mandate a specific transition path such as open source, which may not be the best alternative for a particular technology or performer.

Wait until the last phases of your program to focus on transition.

Source: Law, Organization, and Technology for Enterprise Security and Crime Prevention, SRI, 2018

Concluding Remarks

Successful transition of cybersecurity technology from research to operational use is absolutely necessary to address the rapidly evolving threats, but it is also a difficult endeavor with many challenges. One of the elements of the CNCI and the Strategic Plan for the Federal Cybersecurity Research and Development Program is the Accelerating Transition to Practice (TTP) program. This program recognizes the inherent challenges in technology transition and looks to leverage existing investment in cybersecurity research technologies by further investing in some of the more promising federally-funded technologies in order to facilitate their transition to widespread deployment and use. The goal of this effort is to: (1) identify mature technologies that address an existing or imminent cybersecurity gap in public or private systems that impact national security, (2) identify and fund technology transition opportunities.

Conclusions

This report focuses on three main categories of crime-related issues, putting a particular emphasis on the threats posed by various types of crime. Problems linked to financial (banking, insurance) and energy markets are discussed primarily in relation to cybersecurity, and the authors focus on identifying and describing problems arising on these markets in connection with technological development, the new threats it brings, as well as products and services that are meant to support the activities of various state authorities and services aimed at preventing the causes of crime. In the section on people management, special attention is paid to problems related to possible violations of law linked to particular relations created in the workplace that may lead to abuse, in particular in relation to subordinates, but also among other employees (mobbing, harassment, discrimination).

Cybercrime threats may occur in any sphere of economic and even private life, but certain criminal activities are typical of specific sectors. The report presents an overview of cybersecurity threats and frauds, focusing on the insurance, banking and energy sectors. Then, the report describes a set of concepts and best practices used to deal with significant challenges faced by various institutions in the provision of services in these areas.

The research conducted and made available in this report aims to guide key decision-makers representing financial institutions in shaping the dialogue on implementing best practices in the area of combating fraud and cyberattacks. The report emphasizes the unique nature of cyberspace, as well as the significance of automated methods and infrastructure for creation of a sustainable ecosystem fostering the most effective methods of protection against criminal activities (attack, violation). The section on protection of employees' rights in organizations highlights the significance of compliance, in particular, in ensuring protection of employees and their equal treatment, as well as preventing legal, economic or reputational problems. Particular attention is paid to the issues related to integrating compliance at all the levels of hierarchy.

The issues linked to prevention of psychological and physical violence, and implementation of compliance culture through education, proper leadership or evaluation, are also discussed.

This report also provides information on key technologies shaping the future. The described concepts illustrate the technological development which has completely changed the rules of the game and generated new types of threats. New opportunities in technical domains mean potential new threats as well. Therefore, the report includes the conceptual background of these technologies, as well as an overview of issues related to such important concepts as Big Data, Artificial Intelligence, Cyber Security, and the Internet of Things.



Introduction to the Community Gold Standard



Version 1.1.1

5.2 Capability Areas

The Capability Areas, as indicated by the 11 higher-level boxes in Figure 1, are structured to place complementary Capabilities together to achieve a single IA goal. Each of the Capabilities in an area accomplishes its individual objective while contributing to the overall purpose of the Capability Area.

5.2.1 Know the Enterprise

The Know the Enterprise Capability Area provides the Enterprise with the Capabilities necessary to visualize the network and understand the relationships and connectivity among all devices and their communication, including understanding the interfaces to and interdependencies with other networks and ensuring availability and reliability of resources. It provides the foundational knowledge of the people, facilities, and environmental factors in the Enterprise. It maps the interactions between people, processes, technology, and the environment; identifies the source, destination, and path of all data; and identifies and tracks hardware and software assets.

5.2.2 Protect the Enterprise

The Protect the Enterprise Capability Area provides the Enterprise with the Capabilities necessary to protect the network, its boundaries, and both systems and communications. It provides the ability to screen personnel who may need access to the Enterprise and its resources and prevent unauthorized access to facilities, systems, resources, or information. It establishes and maintains integrity of products and systems through configuration control and ensures that only authorized personnel or systems gain access to and uses Enterprise resources.

5.2.3 Protect Data and Enable Access

The Protect Data and Enable Access Capability Area provides the Enterprise with the Capabilities necessary to protect data in use, at rest, and in transit. It enforces the permissions that define the actions that an entity may or may not perform against a resource; provides, controls, and maintains the cryptographic keys, key material, and key products required to support operational missions; and generates, validates, and maintains IA metadata and metadata schemas. It manages the properties associated with entities in the Enterprise; manages the creation, issuance, maintenance, revocation, and status of identity credentials; and associates identifiers with entities that can perform an action anywhere in the Enterprise. Finally, it generates converts, manages conflicts, validates, provisions, and executes machine-readable policies that enforce the management, use, and protection of Enterprise resources.



Introduction to the Community Gold Standard



Version 1.1.1

5.2.4 Assess the Vulnerability

The Assess the Vulnerability Capability Area provides the Enterprise with the Capabilities necessary to identify potential weaknesses across all susceptible areas. It includes assessment of vulnerabilities in physical, personnel, technological, and environmental protections.

5.2.5 Assess the Threat

The Assess the Threat Capability Area provides the Enterprise with the Capabilities necessary to identify, analyze, and prioritize threat information. Assess the Threat uses data captured by other Capabilities to identify threats and threat sources, understand a threat source's abilities, and determine the probability of the threat exploiting a known vulnerability.

5.2.6 Detect Events

The Detect Events Capability Area provides the Enterprise with the Capabilities necessary to monitor and detect anomalies within the Enterprise systems and the physical infrastructure in order to detect malicious activity. It proactively looks for indicators of an active threat or exploitation of vulnerabilities, provides active and passive monitoring of the Enterprise to share awareness of event changes, and monitors physical and environmental controls to prevent unauthorized physical access to facilities and systems. It also provides assurance that the personnel granted access to facilities, systems, and information have current authorization and clearances. Detect Events identifies, collects, correlates, analyzes, stores, and reports audit information.

5.2.7 Respond to Incidents

The Respond to Incidents Capability Area provides the Enterprise with the Capabilities necessary to establish policy, procedures, and technical measures designed to maintain or restore operations should an incident occur. It enables the Enterprise to prevent host-based and network-based system attacks and provides first line of protection against anomalous activity by responding to signature-based and statistical pattern-based alerts and notifications. It is responsible for analyzing and responding to incidents including triage, escalation, isolation, and restoration of Enterprise functions during and after technical, personnel, physical, and environmental incidents, and for developing, recommending, and coordinating Enterprise mitigation actions provided by the Risk Mitigation Capability.

5.2.8 Manage Risk

The Manage Risk Capability Area provides the Enterprise with the Capabilities necessary to collect and analyze risk-related data. It establishes a relationship between



Introduction to the Community Gold Standard



Version 1.1.1

threat and vulnerability pairs, determines whether these pairs have influence on the Enterprise's risk, decides which mitigations will be applied to the risks, and implements those mitigations. It also assesses the effectiveness of the risk decisions and monitors the current security posture, determining if there are any gaps.

5.2.9 Manage Investments and Portfolios

The Manage Investments and Portfolios Capability Area provides the Enterprise with the Capabilities necessary to understand and effectively budget for the Enterprise's IA resources. It ensures proper planning for and allocation of IA resources, including consideration of technical, personnel, physical, and environmental IA needs. It also ensures the Enterprise follows secure acquisition processes and obtains IA products and services from authorized providers.

5.2.10 Manage the Lifecycle

The Manage the Lifecycle Capability Area provides the Enterprise with the Capabilities necessary to ensure that IA is incorporated throughout the development lifecycle. The Capabilities within Manage the Lifecycle make certain that the necessary security personnel, decision-makers, and stakeholders are included throughout the process to ensure the security requirements are properly defined, approved, tested, and implemented.

5.2.11 Manage Corporate Culture

The Manage Corporate Culture Capability Area provides the Enterprise with the Capabilities necessary to identify, establish, and manage the IA policies, procedures, and standards needed at all levels of the Enterprise to ensure the IA vision and goals can be met. In addition, it establishes the authorities and organizations within the Enterprise responsible for making IA decisions. It defines and manages the training and awareness programs necessary to ensure understanding of the Enterprise IA goals and details proper execution of the IA processes and procedures.

5.3 Composition of the Capability Documents

Each Capability document consists of the following sections. These sections provide an introduction to the content in each document. Within the Capability documents, these sections will be defined within the limitations of current technologies.

5.3.1 Capability Definition

The Definition section of each capability write-up provides a high-level introduction to the Capability. It aids the reader in understanding why the Capability is important to the



Introduction to the Community Gold Standard



Version 1.1.1

Enterprise. It also defines the different parts of the Capability and assists in understanding how the Capability will function within the Enterprise.

5.3.2 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

5.3.3 Environment Pre-Conditions

The Environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

5.3.4 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

5.3.5 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an organization will need to execute or establish to implement the Capability.

5.3.6 Capability Interrelationships

Capability interrelationship maps the Capability within the document to other Capabilities that it either relies on or that rely on it for information, data, monitoring, policies, procedures, standards, alerts, or other functions. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate or influence one another. In many cases there are secondary relationships (not indicated in the mapping), which are provided as a result of the primary relationships.

5.3.6.1 Required Interrelationships

The Required Interrelationships section provides the other Capabilities within the Community Gold Standard framework that are necessary for each Capability to operate.



Introduction to the Community Gold Standard



Version 1.1.1

5.3.6.2 Supporting Interrelationships

The Supporting Interrelationships section provides the other Capabilities within the Community Gold Standard framework that are not necessary for each Capability to operate, although they support the operation of the Capability.

5.3.7 Security Controls

The Security Controls section provides a mapping of each Capability to the appropriate controls. Initially, the mapping will include controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The controls and their enhancements are granularly mapped according to their applicability to each Capability. In some instances, a control may map to multiple Capabilities. The Capability documents are not responsible for providing guidance on implementation of the security controls.

Organizations will be responsible for selecting appropriate security controls, implementing the controls correctly, and demonstrating the effectiveness of the controls in satisfying their stated security requirements. Organizations will be responsible for implementation in accordance with the appropriate Committee on National Security Systems (CNSS), NIST, Department of Defense (DoD), Intelligence Community (IC), or federal/civil policy. In determining which security controls apply to the organization, SP 800-53 and CNSS 1253 can be effectively used to determine applicability and potential impact levels as they potentially affect loss of confidentiality, integrity, or availability within the Enterprise.

The CGS security control mapping does not contain any supplemental guidance or mappings between controls, which are provided in SP 800-53. The implementer should refer to the SP 800-53 for any supplemental guidance and references. They can be found easily by referring to the mapped controls.

5.3.8 Directives, Policies, and Standards

The Directives, Policies, and Standards section identifies existing policies and directives applicable to the Capability. The information provided in this section contributes to the Capability's Gold Standard Guidance, along with other applicable areas. The documents referenced in this section are not agency specific and therefore do not include any directives, policies, or standards that are applicable to only one agency.



Introduction to the Community Gold Standard



Version 1.1.1

5.3.9 Cost Considerations

Although the CGS does not address cost when defining each Capability, it is recommended that the Enterprise consider cost when deciding which Capabilities to implement and to what extent to implement them. In addition to the implementation of the CGS Capabilities, costs associated with related requirements should be considered, including support, documentation, procedures, training, peripherals, communications, and maintenance. Upfront costs as well as ongoing operational, upgrade, and maintenance costs should also be considered. Each Enterprise likely operates in an environment that is unique in its own way. A lot of operating environments will share many similar characteristics, but they will not all have an identical threat level, use identical technologies, and be supported by identical resources. Each Enterprise will adopt CGS Capabilities appropriately in accordance with their mission, operational, and environmental needs based on the resources they have available. Those Enterprises that operate in a high-threat environment will likely want to implement more Capabilities than Enterprises that operate in comparatively low-threat environments.

Cost considerations are factors that involve a tradeoff of limited resources while trying to achieve an objective. Cost considerations also encompass more than just monetary resources. Costs can include all manner of factors including money, time, risk, and opportunity costs. These are factors the Enterprise should consider when they are evaluating the various implementation options for each Capability. Most of the Capabilities share several common cost considerations. In addition, most Capabilities also have some cost considerations that are less common or are completely unique. The Enterprise implementing the CGS will need to consider the cost considerations associated with each Capability in order to estimate the total cost of implementation to effectively evaluate which Capabilities to adopt and how to implement them.

5.3.10 Guidance Statements

The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3 (Capability Gold Standard Guidance) of each of the CGS Capability documents.



CGS Capability Definitions

Version 1.1.1



2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Capability	Definition
Network Mapping	The Network Mapping Capability helps visualize the network and understand relationships and connectivity between all devices and the communications that provide service. Network Mapping is conducting Enterprise-level mapping of all network components. This mapping should depict every network component's network connectivity, at the nodal, logical, and physical level.
	For this Capability, network components shall be defined as every network device connected to the network, whether it has an Internet Protocol (IP) address and whether it is physically connected (shall also include wireless devices).
Network Boundary and Interfaces	The Network Boundary and Interfaces Capability for an Enterprise is essential; it provides for an understanding of the resources' interface to other networks or Enterprises, as well as all the interdependencies involved.
	A network boundary is typically the point at which the resources owned or controlled by an Enterprise stop, and a connection to resources controlled by other entities occurs. Network boundaries are key to ensuring the information assurance (IA) of an Enterprise. Anything inside the network boundary can be controlled, changed, or addressed by the Enterprise; anything outside the network boundary cannot be easily controlled, if it can be controlled at all.
	Networking services and protocols that use open ports or accept incoming connections are considered interfaces. If an interface is directly accessible by systems that are external to the network, that interface is considered an external interface. Directly accessible means this device is on the edge between owned and un-owned resources. Network Boundaries and Interfaces can also be internal

2.1 Know the Enterprise



CGS Capability Definitions



Capability	Definition
	to an Enterprise (e.g., the Enterprise can choose to structure its architecture into a set of distinct networks with defined interfaces among them). This can limit damage and risk, although it often has a negative impact on performance and sharing. If an Enterprise chooses to build internal network boundaries into its architecture, it must be able to identify each boundary and determine what is on each side of that boundary.
	For this Capability, Network Boundaries and Interface components shall be defined as applications, data, and devices connected to both sides of a network boundary (the boundary can be internal (i.e., between enclaves) or external to the Enterprise; however, they may not always be physically connected (e.g., a wireless network interface controller [WNIC] would be one such component).
Utilization and Performance Management	Utilization and Performance Management provides the capability to ensure availability and reliability of resources that directly or indirectly provide support to mission functionality such that they are accessible and usable on demand by an authorized entity. Operations must manage the system to target Utilization and Performance levels to ensure availability and reliability of resources. Specifically, Utilization Management is the directed action to control the use or consumption of organizational resources; Performance Management is the directed action to control and facilitate the accomplishment of a given task.
Understand Mission Flows	 Understand Mission Flows encompasses the definition and articulation of the relationship and dependencies of the mission to the people, process, technology, and environment that directly fulfill or support the missions. Understand Mission Flows provides the capability for the following: Intelligent allocation of resources to establish and maintain functions that fulfill the mission Mission resiliency, i.e., fighting through the attack and service outage, among others Characterization of the mission by its operational status



CGS Capability Definitions

Version 1.1.1



Capability	Definition
Understand Data Flows	Understand Data Flows is the identification and articulation of how the data supports the missions, including identification of the source, destination, and path of the data. It is essential to understand what types of data are being transmitted, processed, or stored and who the end user is of the data. The knowledge provided by Understand Data Flows is important in establishing security policy and protecting data.
Hardware Device Inventory	Hardware Device Inventory provides the Enterprise with the methods and schemas necessary to identify and track its classified and unclassified hardware assets, including operational assets and spares. Maintaining a Hardware Device Inventory means to identify the hardware as well as its components. Hardware shall include components such as network interface cards (NICs), telecom devices, network devices, and hard drives.
Software Inventory	The Software Inventory Capability provides the Enterprise with the methods and schemas necessary to identify and track its software assets. Software may include operating systems, applications, plug-ins, firmware, drivers, and patches.
Understand the Physical Environment	Understand the Physical Environment provides knowledge of the facilities and physical resources being used and provides Enterprise personnel, designated staff, and visitor entry and exit information as well as any interdependencies. Physical Environment includes people, facilities, geographic location, and climate, among other physical considerations.

2.2 Protect the Enterprise

Capability	Definition
System Protection	System Protection is a broader security capability that is focused
	on hardware and software (including applications) hardening and
	enforcement of related protection policies. The goal is to harden
	devices and software appropriately for the operating environment.
	System Protection provides enforcement of policies and practices
	as established in multiple Community Gold Standard (CGS)
	capabilities such as Digital Policy Management, Configuration



CGS Capability Definitions



Capability	Definition
	Management, Access Management, and Port Security. In addition, System Protection is responsible for employing malware defenses.
Communication Protection	Communication Protection is a broad security Capability that is focused on protecting links and routes used for communication and enforcement of related protection policies. The goal is to protect communication channels appropriately for the operating environment. Communication Protection provides enforcement of policies and practices as established in multiple Community Gold Standard (CGS) Capabilities such as Port Security, Network Boundary Protection, Key Management, and Access Management.
Physical and Environmental Protections	Physical and Environmental Protection consists of security in- depth measures (i.e., access controls, cameras, fencing, lighting) that prevent unauthorized access to facilities or resources (i.e., hardware, software); protects resources from natural/unnatural disasters, hazards, and physical and environmental attacks; and encompasses environmental protection, which prevents loss or compromise of facilities, resources, or information resulting from environmental impacts such as temperature, fire, or flood. This Capability allows only people with the proper authorization access to the facilities or information and provides protections for resources even when they are not inside a protected facility (i.e., in the field).
Personnel Security	Personnel Security programs are the first line of defense in protecting personnel, the environment, physical assets, and technology. The Personnel Security Capability provides the security measures necessary to ensure all affiliates are screened prior to being granted access to facilities, systems, and information. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.
Network Access Control	Network Access Control is the capability of the system/network to ensure that each endpoint meets security policies when it connects to the network. The intent of Network Access Control is



CGS Capability Definitions



Capability	Definition
	 to provide technical controls to ensure that only authorized computing platforms gain access to network resources. The Network Access the following: Platform Authentication—Verifies the identity of a platform requesting access to a network Access Policy Compliance—Determines that a platform requesting network access complies with policy for such access Endpoint Policy Compliance—Establishes an endpoint's compliance with applicable configuration, patching, and approved software policy Assessment, Isolation, and Remediation—Isolates platforms not meeting requirements for access from the network and provides for configuration remediation to bring a platform into compliance
Configuration Management	The Configuration Management Capability comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configuration of those products and systems. In addition, Configuration Management starts with the establishment of a baseline and provides management of security features and assurances through control of changes made to hardware, firmware, software, and documentation to protect the information system against improper modifications during the system development lifecycle. Continuous monitoring, remediation, and reporting of system configurations are necessary for a successful Configuration Management program. Configuration Management focuses on Secure Configuration Management and Patch Management to provide assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration Management provides the following focus and capabilities: 1. Secure Configuration Management is the management and control of configurations for an information system with the goal of enabling security and managing risk. Secure



CGS Capability Definitions



Capability	Definition
	 Configuration Management applies the general concepts, processes, and activities of Configuration Management but with a focus on the outcomes that affect the security posture of the information system. Patch Management employs a process to maintain systematic notification, identification, deployment, installation, and verification of operating system (OS) and application software code revisions as well as hardware and firmware. The revisions are known by terms such as updates, patches, hot fixes, and service packs.
Port Security	Port Security helps to control access to logical and physical ports, protocols, and services. This includes all Enterprise devices such as network appliances, servers, workstations, and network boundary devices.
	The Port Security Capability provides the management of logical and physical ports. Port Security management includes deciding which ports, protocols, and services should be available and controlling which services or information may pass to, from, and through the system. This includes making decisions regarding the protection of physical ports and how to lock down services. This Capability also includes an auditing and monitoring function of Enterprise devices to ensure compliance with Port Security policies.
Network Boundary Protection	Network Boundary Protection is the Capability to protect and control access to Enterprise resources across a security boundary. A security boundary exists when there is a separation of entities (systems, networks, enclaves, or Enterprises), which are governed by differing security policies or operate in a different threat environment. Network Boundary Protection is carried out by placing information assurance (IA) mechanisms between the internal system and the systems external to the security boundary. Examples of such IA mechanisms include, but are not limited to, Cross-Domain Solutions (CDSs), Controlled Interfaces, Demilitarized Zones (DMZs), Virtual Private Networks (VPNs), and encryption devices at the boundary, or interface. Because of



CGS Capability Definitions



Capability	Definition
	the differing nature of boundary protection devices, a brief explanation of the example technologies is provided here for completeness.
	The purpose of a CDS is to provide a manual or automated means for transferring data between two or more differing security domains. The CDS is responsible for ensuring that unauthorized information cannot leak from a domain with information controlled at a higher level (e.g., classified information) to a domain that is controlled at a lower level (e.g., unclassified information). The CDS is also responsible for protecting the network from malicious content that may be passed from the less controlled network. CDSs enable the transfer of information among security domains, which is normally prohibited by automated policies, but is required for successful completion of a mission.
	The purpose of a Controlled Interface is to control access and information flow into and out of the domain. A Controlled Interface is used when the security policy between interconnected domains is fairly similar. In this instance, the networks are at the same classification level and the risk of contamination or attack by another domain is considered to be sufficiently low.
	The purpose of a DMZ is to provide an additional layer of security to an Organization's network when some of its services must be exposed to a larger community. A DMZ can be a physical or logical subnetwork. With a DMZ, the Organization can provide an external face and external services, while controlling interactions with the internal network and ensuring that an external attacker is restricted to the equipment in the DMZ, rather than having access to any part of the internal network.
	The purpose of a secure VPN (not a traffic engineering VPN) is to provide a connection into the network from a remote point, either for a user to gain access or to establish a connection between two networks. To perform this function, the VPN establishes a relationship between the endpoints (through authentication mechanisms) and then encrypts traffic between those endpoints



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	such that traffic is protected from the underlying network.

2.3 Protect Data and Enable Access

Capability	Definition
Identity Management	Identification is the means by which a user provides a claimed identify to the system. The most common form of identification is the user ID. A user ID is a unique identifier, such as a character string, used by an information system to identify a specific user. An identifier is a representation of a person (or non-person entities) on a network. A person or non-person entity can have more than one identifier. Identify Management is the function that unambiguously associates identifiers with entities such as individuals, Organizations, Communities of Interest (COIs), automated processes, and devices—anyone or anything that can perform an action anywhere in the Enterprise system. Identity Management is the underpinning for building trust in a need-to-share Enterprise model, where entities in any environment (stable to austere), and from any location within an Enterprise system, will be able to access information, services, and communications resources based in large part on an authenticated identity. The Identity Management function provides the Enterprise with the ability to create, issue, distribute, maintain, archive, and manage the lifecycle of globally unique identifiers, as well as to serve as an authoritative source of identity information.
Access Management	 Access management enforces the policies that define the actions that an entity may or may not perform against a resource. The Access Management Capability provides criteria that are used to make an access decision and the rules that will be used to assess those criteria. Specifically, Access Management will validate access through these fundamental steps: Authentication–Validating the identity of an entity within the system. Authorization–Determining the rights of the entity with


CGS Capability Definitions



Capability	Definition
	 respect to a resource. 3. Enforcement–Ensuring that an entity can access only the resources for which it is authorized based on authorization and resource access policies. Access management includes controlling access to physical spaces in addition to access to technology and electronic
	systems.
Key Management	Key Management is a service and process that provides, controls, and maintains the cryptographic keys, key material, and certificates required to support a wide range of operational missions. This Capability governs the key lifecycle, which includes key registration, ordering, generation, distribution, usage, expiration, revocation, and destruction. In addition, Key Management includes the functions of compromise management, accounting, handling, audit, and storage.
Digital Policy Management	Digital Policy Management consists of a set of functions used to generate, convert, deconflict, validate, assess effectiveness, provision for distribution and deployment, and execute machine- readable policies used to enforce how resources are managed, used, and protected. These policies may include rules for authentication (e.g., trusted authorities, criteria for determining authenticity), system configurations, access rules, authorized sources of record or sources of reference, transport connectivity, bandwidth allocation and priority, audit event collection, and computer network defense monitoring and response (e.g., course of action).
	The Digital Policy Management Capability refers to digital policy as expressed in machine-executable form so that it can be directly implemented in systems without human intervention. Non- digital policy is policy that is encapsulated in human language (even if the policy is captured in a "digital form"). Non-digital policy is covered in the IA Policies, Procedures, and Standards Capability.



CGS Capability Definitions



Capability	Definition
Metadata	Metadata is data about data. It is used to describe characteristics
Management	 of data assets to enhance their value and usability. There are many different types of metadata. Some of these types include the following: Discovery metadata—Helps entities find data assets Mission metadata—Describes data assets in their mission context Information assurance (IA) metadata—Encompasses any metadata associated with the protection of a data asset. This can include metadata describing a data asset's security properties, protection requirements, applied protections, and provenance (source of an entity). IA metadata enables data consumers to assess the trustworthiness of the data, while allowing providers to specify controls for their data.
	IA Metadata Management is the maintenance of IA metadata schemas and the generation, validation, association, and maintenance of IA metadata. The management of IA metadata specifically is the focus of this Capability.
	IA metadata is needed to realize information sharing objectives. Assured information discovery and retrieval hinges on resource attributes that can be conveyed in IA metadata and are sharable across domains. IA metadata supports interoperability for human understanding of data assets and for processing by automated systems, such as discovery services and access control functions. To fully realize interoperable secure information exchange, Enterprises must adhere to the following: a common and consistent Community-approved controlled IA vocabulary (i.e., standard meaning and vocabulary for security or sensitivity markings, specification of format for IA metadata, specification of subject roles and attributes), a robust information sharing infrastructure to protect both data assets and IA metadata, and a set of tools and protocols that facilitates the adoption of IA metadata standards (e.g., cryptographic binding, IA metadata validation) within and across Enterprise boundaries.



CGS Capability Definitions



Capability	Definition
	IA metadata supports the assessment of the authoritativeness and trustworthiness of data assets that are used by mission supporting entities. This provides the information needed for continuing protection of those data assets. Trustworthiness assessment includes identifying the extent to which the data asset should be protected from unauthorized disclosure and from unauthorized or unintentional modification while being processed, stored, or exchanged. The IA metadata and the use of IA for metadata and data assets can be afforded the same authoritativeness and trustworthiness as the data asset, and thereby be relied on to formulate decisions.
	Like all data, IA metadata needs to be protected using appropriate data protection techniques. IA metadata can be embedded within a data asset, stored alongside a data asset, or stored separately from its associated data asset (e.g., in a repository). Regardless of where IA metadata is stored, all security protections must still apply, such as those provided under the System Protection, Data Protection, and Communications Protection Capabilities, among others.
Credential Management	A credential is means of providing evidence that supports a claim of identity, assertion, or association. Credential Management encompasses the functions to manage the creation, issuance, maintenance, revocation, reissuance, and status of each credential. Credentials are used as part of the authentication process, and
	authentication focuses on confirming a person's (or non-person's) identity, based on the reliability of his or her credential.
	 There are two types of individual authentication: a) Identity authentication–Confirming a person's unique identity. b) Attribute authentication–Confirming that the person belongs to a particular group or function (such as military veterans or U.S. citizens). For purposes of this Capability, Credential Management refers to



CGS Capability Definitions



Capability	Definition
	identity credentials only. For information on management of attributes (and application of attribute credentials), see the Attribute Management Capability.
	Identity authentication can be conducted using credentials such as certificates and passwords. Certificates are digitally signed representations of an identity that are issued by a trusted authoritative source. For certificate-based credentials, the certificate is presented to support authentication. For non- certificates, such as passwords, authentication is completed by confirming that the credential applies to the user (the credential itself is the linkage between the account and the password).
Attribute Management	The Attribute Management Capability is responsible for managing the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies. Examples of some possible attributes are contact attributes (email address, phone number), demographic attributes (organization, affiliation), and device attributes (physical location, logical addresses, installed software, and patch level).
	Attribute Management encompasses the functions that manage the identification, maintenance, and publication of each attribute. In addition, Attribute Management identifies the attributes that are needed and an authoritative source from which to retrieve the attribute values.
	A given attribute may be dynamic or static, which is determined by the authoritative source. Attribute Management provides for a capability in which all attributes stored by any system on a network are controlled by a set of policies to restrict or enable access based on functional need.
Data Protection	Data protection is protecting all data so that it is available when requested and only authorized users may access, modify, destroy, or disclose the data. Data protection is enforced in all data states including in use, at rest, and in transit. Data in use



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	refers to data that is being acted upon. Data at rest refers to data
	that is being stored. Data in transit refers to data being transferred between systems.

2.4 Assess the Vulnerability

Capability	Definition
Network Security Evaluations	Network Security Evaluations are comprehensive examinations of a network, its architecture, and its defenses. They are used to identify strengths and weaknesses in a given network and provide recommendations for correcting the problems that are identified.
	 Network Security Evaluations are used by Organizations to accomplish several objectives: Identify vulnerabilities in operational systems Measure the effectiveness of security policy and effect changes Demonstrate the impact of network vulnerabilities when attacked
	Network Security Evaluations are commonly conducted in two parts, where each part takes a different approach to assessing the network. One approach is to attempt to infiltrate the system by emulating an adversary. The other approach is to conduct the evaluation in cooperation with the local network and system administrators to review the security policies, protections, and network architecture. Network Security Evaluations identify vulnerabilities that exist within a network and provide feedback to the network owners, identifying those vulnerabilities, making recommendations for mitigation, and stating their mission impact.
Architecture Reviews	The Architecture Reviews Capability establishes Architecture Reviews, which are requirements-based reviews to determine whether the requirements were satisfied by the architecture. Security Architecture Reviews focus specifically on determining whether the security requirements for a system, application, or service were included in the architecture (sometimes called



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	security architecture). The reviews demonstrate security requirement satisfaction as well as potential vulnerabilities as a result of missing requirements. The review may be conducted on logical (e.g., data flows) or physical (e.g., physical connections) architectures.
Vulnerability Assessment	A vulnerability is a weakness that has the potential to reduce an Enterprise's ability to fulfill its mission. Vulnerability Assessment is the systematic examination of an Enterprise to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Vulnerability alerts are released to initiate follow-on functions

Capability	Definition
Threat	The Threat Assessment Capability identifies, analyzes, and
Assessment	prioritizes threat information by identifying threats and threat sources, understanding the threat's capability, and determining the likelihood of the threat occurring.
	A threat is the potential for a particular threat source (or set of threat sources) to successfully exploit a particular vulnerability (or set of vulnerabilities) that has the potential to adversely impact agency, agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
	A threat source is either 1) the intent and method targeted to intentionally exploit a particular vulnerability (or set of vulnerabilities) or 2) a situation and method that may accidentally overwhelm a vulnerability (or set of vulnerabilities). Common threat sources include, but are not limited to, natural threats such as floods, earthquakes, and tornadoes; human threats such as terrorists, computer criminals, and insiders; and environmental

2.5 Assess the Threat



CGS Capability Definitions

Version 1.1.1



	threats such as long-term power failure, chemicals, and pollution.
	A threat capability is the level of access, resources, knowledge, and skill that a threat source is capable of applying against technical, personnel, physical, and environmental aspects of the Enterprise. The threat likelihood is the probability of a given threat source's attempt to exploit a given vulnerability.
Signature	A Signature Repository Capability provides a group of signatures
Repository	for use by network security tools such as anti-virus applications, host or network sensors that require signatures (e.g., intrusion detection/prevention systems), and other monitoring and detection applications. For analysis, the Organization uses these signatures to understand the attack patterns and their relationship to specific threats or activities.

2.6 Detect Events

Capability	Definition
Network	The Network Enterprise Monitoring Capability employs active and
Enterprise	passive monitoring of the network on an Enterprise level to detect
Monitoring	security- or performance-relevant changes or events. This includes continuously monitoring the state of the network and networked devices across the Enterprise to share awareness of event changes. It also includes monitoring health and status, links between devices, and traffic flow. Enterprise-level monitoring is used to provide inputs to the overall situational awareness picture.
Physical	Physical Enterprise Monitoring is the monitoring of the physical
Enterprise	and environmental controls that prevent unauthorized physical
Monitoring	access to facilities, systems, or other resources. This Capability includes the monitoring of the environment, systems, hazards, and other resources; it ensures that the physical and environment protection systems are still effective when changes occur.
Personnel	Personnel Enterprise Monitoring is the monitoring of the
Enterprise	personnel mechanisms and processes that prevent unauthorized
Monitoring	access to facilities, systems, and information. The Personnel Enterprise Monitoring Capability provides assurance that the



CGS Capability Definitions



Capability	Definition
	affiliates granted access to facilities, systems, and information have proper authorization and clearances and follow information assurance (IA) policies and practices. The Personnel Enterprise Monitoring Capability establishes and executes the ongoing procedures that occur after the initial personnel security verifications, which provide a basis for granting access. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.
Network Intrusion	The Network Intrusion Detection Capability helps to detect
Detection	malicious activity incoming to, outgoing from, and on the network. Network Intrusion Detection Systems are deployed to inspect all network traffic for malicious activity, including anomalies and incidents. The network traffic is examined by passive and in-line computer network defense sensors located within the network.
Host Intrusion Detection	The Host Intrusion Detection Capability helps to detect malicious activity by monitoring for anomalies within the system that indicate malicious activity. The Capability is deployed to monitor the internals of a system(s) for threats.
Network Hunting	The Network Hunting Capability is employed to proactively look for indicators of an active threat or exploitation of a vulnerability that was previously known or unknown. Network Hunting may involve signature detection and detection of changes in behaviors and normal usage, as well as the ability to detect incidents that are not known to be occurring.
Physical Hunting	Physical Hunting is employed to detect anomalies in the physical components, and vulnerabilities associated with those components, in the physical infrastructure of the Enterprise. Physical Hunting may involve detection of technical surveillance devices (e.g., keystroke taps, bugs). This Capability provides for hardware forensics and searching for vulnerabilities in the physical Enterprise, including intended emanations and changes to the environment.
Enterprise Audit	The Enterprise Audit Management Capability involves the identification, collection, correlation, analysis, storage, and



CGS Capability Definitions

Version 1.1.1



Capability	Definition
Management	reporting of audit information, and monitoring and maintenance of the Capability. An Enterprise Audit Management solution should be deployed to centralize audit collection and provide appropriate storage for and access to audit data. For each type of audit (specific to system/mission/data), auditable events are identified, auditing is conducted to properly capture and store that data, and analysis and reporting are performed. Certain high-profile events should trigger automated notification to individuals such as systems administrators.

2.7 Respond to Incidents

Capability	Definition
Incident	Incident Response is a conscious plan of action given the
Response	stimulus of an assessed occurrence having actual or potentially adverse effects on an asset. It involves notification, triage, escalation, isolation, and restoration (when appropriate) of technical, personnel, physical, and environmental incidents. Incident Response provides the Capability to respond to any incident (both external to the network and information technology [IT] related). A formal Incident Response Team (IRT) provides the expertise to appropriately respond to the problem.
Incident Analysis	Incident Analysis uses information gathered during Incident Response to determine the root cause of an incident. The Incident Analysis generated is used to develop, recommend, and coordinate Enterprise mitigation actions for technical, personnel, physical, and environmental incidents.
Network Intrusion Prevention	Network Intrusion Prevention employs a response to perceived anomalous activity on the network. When this activity is perceived, Network Intrusion Prevention encompasses mechanisms to react to block, drop, redirect, and/or quarantine anomalous activities. Network Intrusion Prevention is enabled through network-based modules deployed throughout the network.



CGS Capability Definitions

Version 1.1.1



Capability	Definition
Host Intrusion Prevention	The Host Intrusion Prevention Capability employs a response to a perceived incident of interference on a host-based system and encompasses mechanisms that reside on a host to react in real- time to block, drop, redirect, and/or quarantine malicious activities. Host Intrusion Prevention is enabled through a host-based system rather than on a network appliance.
Contingency Planning	Contingency Planning establishes policy, procedures, and technical measures designed to maintain or restore business operations. This includes computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disasters. Contingency Planning occurs under all circumstances, including major disasters and events.
	The Contingency Planning Capability focuses on Information System Contingency Planning, which refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-34). The purpose of Information Systems Contingency Planning is to ensure the business and mission functions of an Organization under all circumstances.

2.8 Manage Risk

Capability	Definition
Risk Identification	Risk Identification is the creation of a relationship between the results of the Threat Assessment and Vulnerability Assessment Capabilities. It establishes the influence that the threats and vulnerabilities are perceived to have on the Enterprise's risk.
	The risk-related data comprises known threats and vulnerabilities and their combined impact. With this in mind, a simple notional function that demonstrates the relative relationships between Risk, Threat, Vulnerability, and Impact is $R = f(T,V,I)$ as represented by a portfolio of attacks. The impact portion of the



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	relationship is determined in the Risk Analysis Capability.
Risk Analysis	The Risk Analysis Capability collects and analyzes risk-related data from the Risk Identification Capability for the broader purpose of providing decision-makers information on the benefits, costs, and uncertainty of alternative courses of action with respect to executing the assigned mission in multiple environments. The risk-related data comprises known threats and vulnerabilities and their combined impact. With this in mind, a simple notional function that demonstrates the relative notional relationships between Risk, Threat, Vulnerability, and Impact is $R = f(T,V,I)$, as represented by a portfolio of attacks. The threat and vulnerability information is aggregated from the Threat and Vulnerability Assessment Capabilities during the risk identification process in the Risk Identification Capability.
Risk Mitigation	Risk Mitigation is the reduction of the likelihood and/or impact of Enterprise security risk. The Risk Mitigation Capability decides which mitigations will be applied to identified risks, implements those mitigations, and subsequently reduces the risk level.
Risk Monitoring	Risk Monitoring assesses the effectiveness of the risk decisions that are made by the Enterprise. This Capability establishes the current security posture and then determines the gaps between the current security posture and the intended risk posture (see the Risk Analysis Capability). Risk Monitoring includes the monitoring of risks (as identified in the Risk Identification Capability) pertaining to people, operations, technology, and environments. Risk levels must be monitored based on changes in the risk posture.

2.9 Manage Investments and Portfolios

Capability	Definition
Finance	Finance is an integral part of the Organization's process for
	obtaining funds for the procurement of information assurance (IA)
	services and products in line with the Organization's current



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	budget. The Finance Capability ensures that Organizations have budgeted for IA programs, products, and services throughout the Enterprise. The budget includes funding for personnel, operational, environmental, and technical considerations, as well as funding for enabling supporting resources such as IA training and recruitment.
Acquisition	The Acquisition Capability provides supply chain risk management by determining an appropriate risk management approach for individual acquisitions of products and services. The Acquisition Capability provides research and analysis of suppliers and products and provides that information to the Risk Analysis Capability to make a risk decision regarding whether risks associated with a product or service can be properly managed by the Enterprise. These measures provide assurance against products having intentional security flaws, supplier personnel posing unknown vulnerabilities, or other risks that may be unacceptable to the Enterprise.
Portfolio Management	Portfolio Management is the process of analyzing, selecting, controlling, and evaluating Capability needs against current and planned investments within a Capability portfolio to better inform decision-makers and optimize resources. Portfolio Management involves the alignment of programs, initiatives, and activities with Enterprise priorities and requirements to maximize the return on investment. This Capability is specifically concerned with information assurance (IA) Portfolio Management, which is focused on the alignment of IA programs, initiatives, and activities. This information will feed into the Enterprise's overall Portfolio Management Capability efforts.

2.10 Manage the Lifecycle

Capability	Definition
Development	Development is the creation of a solution based on an identified
	need. The development phase of the lifecycle comprises many
	activities that ensure that information assurance (IA) is included



CGS Capability Definitions

Version 1.1.1



Capability	Definition
	from concept up to the Deployment Capability. The Development Capability includes the incorporation of IA during architecture, concept, design, implementation/build, integration, requirements, and test.
Deployment	Deployment is the phase of the system development lifecycle in which solutions are placed into use to change or maintain the operational baseline. The Deployment Capability ensures that information assurance (IA) is employed while the processes for deployment are executed. When necessary, Deployment includes integration into the environment or other solutions and testing within that environment.
Operations and Maintenance	The Operations and Maintenance Capability encompasses the activities of the Operations and Maintenance phases of the system development lifecycle. These activities include technical and administrative procedures that account for the use and maintenance of hardware, software, and data assets that support the mission. The Operations and Maintenance Capability shall employ an approved system development lifecycle process (established in accordance with the IA Policies, Procedures, and Standards Capability) that implements and maintenance.
Decommission	The Decommission Capability includes the execution of technical and administrative procedures prior to, during, and following removal and disposal of hardware, software, and data assets. During decommission, approved procedures are employed, which maintain information assurance (IA) and prevent the inadvertent compromise of data. This may include sanitization, declassification, and additional releasability procedures.

2.11 Manage Corporate Culture

Capability	Definition
IA Policies,	The Information Assurance (IA) Policies, Procedures, and
Procedures, and	Standards Capability encompasses existing policies, procedures,



CGS Capability Definitions



Capability	Definition
Standards	and standards and defines, distributes, stores, implements, enforces, reviews, and maintains them, as needed. IA Policies, Procedures, and Standards are defined by an Organization in accordance with national, Department of Defense (DoD), and Intelligence Community (IC) policies. These policies, procedures, and standards may be used in identifying and establishing subsequent policies, procedures, and standards for IA. Organizations may use a variety of terminology in their internal structure to refer to policies, procedures, and standards.
	Policies regulate, direct, or control actions for the Organization. They generally provide broad statements, assign responsibilities and authorities, and identify the applicable policy source and references.
	Procedures provide specific implementations for the policy, which may assign further responsibility and implementation guidance. Procedures tend to be written at a lower level than policies and contain more specific information about what actions are required.
	Standards include establishment of the corporate vision and strategy, Enterprise operations, and governance. They define the mission statement and goals. At the lower level, standards also define corporate or technical best practices (a subset of policies and procedures). Standards that are defined based on the needs of the Organization can also be used to generate IA policy and procedures.
IA Awareness	The Information Assurance (IA) Awareness Capability promotes understanding of IA objectives, threats, risks, and actions, among other IA concerns. IA Awareness is intended to empower individuals to recognize IA or security concerns and respond accordingly.
IA Training	Information Assurance (IA) Training is the training of users and IA practitioners on IA policies, requirements, processes, and procedures. It also includes technical and operational IA Training to all personnel based on user and/or role. Within this Capability, an IA Training program is established, which includes



CGS Capability Definitions



Capability	Definition
	identification, administration, maintenance, and evaluation of the training activities and materials.
Organizations and	The Organizations and Authorities Capability encompasses the
Authorities	definition, establishment, governance, and revocation of information assurance (IA) roles and responsibilities within the Enterprise and provides for their continued authorization. These roles and responsibilities include personnel, physical, environmental, and technology considerations. Roles are responsible for executing and enforcing the IA vision of the Organization and ensuring that the definition and execution of projects and programs are aligned with the Community Gold Standard (CGS) Framework.
	The Organizations and Authorities Capability also provides accountability for reporting and performing roles, defining Organizations, and making decisions. In addition, Organizations and Authorities facilitate the collaboration and coordination of operations across different authorities and organizational boundaries.

Appendix 3. Community Gold Standard Best Practices Tool Kit (Link) page 1

The set of detailed documents are over 1000 pages of materials. Below is a visual of the set and, for practical purposes, a (sharable) Google Drive link with all the materials has been sent

https://drive.google.com/drive/folders/1TMiguWkpQSjxByA3PIVO398D0zJigJ7P?usp=sharing

Network_Mapping_v1.1.1.pdt
Software_Inventory_v1.1.1.pdf
Understand_Data_Flows_v.1.1.1.pdf
Understand_Mission_Flows_v1.1.1.pdf
Understand_the_Physical_Environment_v1.1.1.pdf
Utilization_and_Performance_Management_v1.1.1.pdf
Assess the Threat
Signature_Repository_v1.1.1.pdf
Threat_Assessment_v1.1.1.pdf
Assess the Vulnerability
Architecture_Reviews_v1.1.1.pdf
Network_Security_Evaluations_v1.1.1.pdf
Vulnerability_Assessment_v1.1.1.pdf
CGS Acronyms_v1.1.1.pdf
CGS_Capability_Definitions_v1.1.1.pdf
CGS_Framework_v1.1.1.pdf
Detect Events
Enterprise_Audit_Management_v1.1.1.pdf
Host_Intrusion_Detection_v1.1.1.pdf
Network_Enterprise_Monitoring_v1.1.1.pdf
Network_Hunting_v1.1.1.pdf
Network_Intrusion_Detection_v1.1.1.pdf
Personnel_Enterprise_Monitoring_v1.1.1.pdf
Physical_Enterprise_Monitoring_v1.1.1.pdf
Physical_Hunting_v1.1.1.pdf
Introduction_to_CGS_v1.1.1.pdf
Know the Enterprise
Hardware_Device_Inventory_v1.1.1.pdf
Network_Boundary_and_Interfaces_v1.1.1.pdf

▼	Manage Investments and Portfolios
	Acquisition_v1.1.1.pdf
	Finance_v1.1.1.pdf
	Portfolio_Management_v1.1.1.pdf
▼	📃 Manage Risk
	Risk_ Analysis_v1.1.1.pdf
	Risk_Identification_v1.1.1.pdf
	Risk_Mitigation_v1.1.1.pdf
	Risk_Monitoring_v1.1.1.pdf
lacksquare	Manage the Lifecycle
	Decommission_v1.1.1.pdf
	Deployment_v1.1.1.pdf
	Development_v1.1.1.pdf
	Operations_and_Maintenance_v1.1.1.pdf
▼	Protect Data and Enable Access
	Access_Management_v1.1.1.pdf
	Attribute_Management_v1.1.1.pdf
	Credential_Management_v1.1.1.pdf
	Data_Protection_v1.1.1.pdf
	Digital_Policy_Management_v1.1.1.pdf
	Identity_Management_v1.1.1.pdf
	Key_Management_v1.1.1.pdf
	Metadata_Management_v1.1.1.pdf

Appendix 3. Community Gold Standard Best Practices Tool Kit (Link) page 2

Appendix 3. Community Gold Standard Best Practices Tool Kit (Link) page 3 https://drive.google.com/drive/folders/1TMiguWkpQSjxByA3PIVO398D0zJigJ7P?usp=sharing

▼	Protect the Enterprise
	Communication_Protection_v1.1.1.pdf
	Configuration_Management_v1.1.1.pdf
	Network_Access_Control_v1.1.1.pdf
	Network_Boundary_Protection_v1.1.1.pdf
	Personnel_Security_v1.1.1.pdf
	Physical_and_Environmental_Protections_v1.1.1.pdf
	Port_Security_v1.1.1.pdf
	System_Protection_v.1.1.1.pdf
▼	Respond to Incidents
	Contingency_Planning_v1.1.1.pdf
	Host_Intrusion_Prevention_v1.1.1.pdf
	Incident_Analysis_v1.1.1.pdf
	Incident_Response_v1.1.1.pdf
	Network_Intrusion_Prevention_v1.1.1.pdf

Appendix 4 – Insurance Europe: Combating fraud (1)

What is the industry doing to combat fraud?

The insurance industry's responses to fraud vary between countries and the initiatives are wide-ranging. For instance:

- In several countries, insurers exchange relevant information to help them identify potential frauds. Insurers are transparent about this and operate in compliance with data protection and privacy requirements. Such exchanges of information among insurers (in varying forms) exist in Croatia, Estonia, Finland, Germany, Ireland, Malta, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden and the UK, and are currently being considered in Cyprus.
- **Cross-border cooperation** also exists. For example, the Nordic countries meet regularly to discuss trends, issues and common challenges, since trends in one country have been seen to spread to neighbouring countries.
- In several countries, including France, Sweden and the UK, insurance companies have set up (more or less) formalised groups to investigate insurance fraud.
 - In France, insurers set up a national body (Agence pour la lutte contre la fraude à l'assurance, ALFA) in 1989 to investigate suspicious claims. ALFA aims to promote counter-fraud activities, drawing up suitable tools to assist the industry in combating fraud. These include: training and certification of fraud investigators, advice on how to handle fraudulent cases that target several insurers at a time, and advice on managing relationships with law enforcement agencies.
 - In Sweden, insurance undertakings have created special investigation units that are charged with detecting insurance fraud. Insurance Sweden encourages these units to make police reports of detected or suspected frauds.
 - In the UK, the Insurance Fraud Bureau (IFB) focusses on detecting and preventing organised and cross-industry insurance fraud. The IFB leads or co-ordinates the industry response to the identification of criminal fraud networks and works closely with the police and other law enforcement agencies. It encourages and helps people to report suspected or known frauds anonymously through an insurance cheat-line. The impact of the IFB has been hugely positive since its launch in July 2006, with numerous arrests and tens of millions of pounds of savings for insurers and ultimately their customers.

Appendix 4 – Insurance Europe: Combating fraud (2)

- Insurers have also increased their co-operation with law enforcement agencies in several countries. This is the case, for example, in Croatia, Denmark, Estonia, Germany, Ireland, the Netherlands, Portugal, Spain, Sweden and the UK.
 - Evidence from several law enforcement agencies shows that many are unaware of the simple visual checks that can be made to identify possible stolen private or commercial vehicles. International efforts to train law enforcement staff have been initiated by Europol, Interpol and national insurance associations.
 - In Denmark, insurers are urged to report every documented fraud to the police. F&P organises exercises at the Danish Police Academy on how to combat insurance fraud. Former police officers are often employed in the insurance industry to assist with detection and evidence-gathering.
 - In Croatia, the insurance association initiated a Protocol on Cooperation to Combat Insurance Fraud in 2002. The Protocol formalises cooperation both between insurers and between insurers and third parties such as the police, the judiciary and other agencies. The Protocol has an international reach and is signed by several other national insurance associations in the region, including Austria, the Czech Republic, Slovenia and Hungary.
 - In the UK, the Insurance Fraud Enforcement Department (IFED) is funded by insurers. Set up in January 2012, it forms part of the City of London Police, the UK's lead police force for economic crime and insurance fraud. It investigates potential frauds referred by insurers in all types of insurance. In its first nine months of operation, IFED made over 200 arrests with £12m (€14m) of suspected insurance fraud under investigation.
 - In Spain, almost all insurance undertakings have appointed fraud representatives. These representatives have access to a confidential extranet containing data from the police about current investigations.
- Insurers increasingly use technology to uncover fraud. Methods include electronic devices to detect the authenticity of documents submitted in support of claims and the use of publicly available information on various social media and other websites.
 - In Sweden, insurance undertakings use advanced key-readers to confirm that car keys submitted in support of a claim for a stolen vehicle are those belonging to the car alleged to have been stolen.

Appendix 4 – Insurance Europe: Combating fraud (3)

- In the UK, a claim for alleged back injuries was rejected when Facebook images showed the claimant performing gymnastics and training for a charity run.
- **Training** of insurance staff and police is widely used to raise awareness of fraud, to show how to detect it and to highlight the new and ever-changing methods used by fraudsters.
 - In Denmark, F&P organises seminars on insurance fraud for its members. Seminars are aimed at general insurance fraud, but can also be tailored to specific areas, such as car immobilisers and car keys, luggage handling at airports, fraud via internet freight exchange, codes of ethics for investigators, fraud in household content insurance and so on. Training is provided to those working in fraud detection, including insurance investigators, chief claim handlers and specialist claim handlers.
 - In Germany, annual training is given to claims adjusters to teach them how to detect and combat fraud. The training is conducted by practitioners from the insurance industry, legal advisors, technical specialists, police experts and medical scientists. Participants can take an exam to acquire a certificate of expertise in detection.
 - In the UK, bodies like the IFB and IFED run specialist workshops for counter-fraud staff, and many insurance companies additionally run training schemes at induction and throughout employees' careers and appoint "fraud champions" who emphasise and remind colleagues of the possibility of fraud in all areas of the business.
 - In Finland, the insurance federation has been organising seminars and training with the police, other authorities and the media for 30 years.
- The use of **"cheat-lines"** is successful in several countries, including Ireland, Sweden and the UK. Members of the public can call a helpline to report suspected or known insurance fraud. The caller will generally retain anonymity to encourage such reporting.
 - In Ireland, a man obtained motor insurance with an insurance company. On the proposal form he completed to obtain the insurance, he stated that he had no previous motor convictions. However, the insurance company received an anonymous tip-off via the insurance federation's Insurance Confidential hotline that the man had several motor convictions. The insurer's internal investigation team carried out further investigations, which resulted in the matter being passed to the police. The individual was subsequently convicted for obtaining insurance by making a false declaration and driving without insurance. He received a four-month suspended sentence.

Appendix 5 – Deloitte Case Study (1)

Case 1 – Hackers steal personal data about customers – and potential customers

Organization

A group of large insurance and financial services companies.

Scenario

Cyber-criminals breached the company database and stole information of more than one million customers and sales prospects, including driver's license data and social security numbers.

Attackers and motivation

Cyber-criminals were after personal identifiable information in order to sell it on the black market for identity fraud purposes.

Techniques used

Part of the network used by the organization's members was breached by cybercriminals and used to steal customer information.

Business impact

The organization was obliged to provide affected customers with free credit monitoring for a year, and to reimburse all damages resulting from the breach. In addition to those tangible costs – which were substantial – the organization suffered significant brand damage and loss of trust. Appendix 5 – Deloitte Case Study (2)

Case 2 – Even small breaches can have a meaningful impact and require corrective action

Organization

A very large investment and insurance company.

Scenario

The attack targeted company employees with e-mails containing malware that could capture confidential data such as bank account numbers, social security numbers, user accounts/logins, passwords and credit card numbers. Hackers used this information to compromise several servers, including servers used by employees to remotely access the company's IT systems.

Attackers and motivation

Cyber-criminals were after online banking information to perpetrate fraud for financial gain.

Techniques used

The attack targeted company employees with e-mails containing malicious software that could capture confidential data such as bank account numbers, social security numbers, user accounts / logins, passwords and credit card numbers.

Business impact

Although the attack affected only a small number of employees – and only a handful of customers – it still received media coverage that damaged the company's reputation.

Appendix 5 – Deloitte Case Study (3)

Case 2 -Targeted insurer accused of doing too little too late

Organization

An insurance and financial services firm that specializes in serving seniors.

Scenario

Attackers exploited vulnerable software on the company's servers and stole payment card information for more than 93,000 customers, including names, addresses and unencrypted card security codes.

Attackers and motivation

Cyber-criminals were after payment card information to sell on the black market and commit fraudulent transactions.

Techniques used

Vulnerabilities in the company's systems and software were discovered and exploited by the cybercriminals to gain access to payment card information.

Business impact

The company immediately removed the vulnerable IT elements and had to issue a formal apology. It also offered free identify fraud monitoring to affected customers. However, the company has been strongly criticized for retaining unencrypted security codes – which is a noncompliance issue according to the Payment Card Industry Data Security Standard (PCI DSS) – and for not reporting the breach to its customers sooner.

Appendix 6 – 2015 NAIC Roadmap for Cybersecurity Consumer Protections (1)



Attachment C-Two Executive (EX) Committee and Plenary 12/17/15

PROPOSED AMENDMENTS

Cybersecurity Bill of Rights

NAIC Roadmap for Cybersecurity Consumer Protections

This document describes the protections the NAIC believes consumers are entitled to from insurance companies, agents and other businesses when they collect maintain and use your personal information, including what should happen in connection with a notice that your personal information has been involved in a data breach. Not all of these consumer protections are currently provided for under state law. This document functions as a Consumer Bill of Rights and will be incorporated into NAIC Model laws and regulations. If you have questions about data security, a notice you receive about a data breach, or other issues concerning your personal information in an insurance transaction, you should contact your state insurance department to determine your existing rights.

As an insurance consumer, you have the right to:

- 1. Know the types of personal information collected and stored by your insurance company, agent or any business they contract with (such as marketers and data warehouses).
- 2. Expect insurance companies/agencies to have a privacy policy posted on their website and available in hard copy, if you ask. The privacy policy should explain: what personal information they collect, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency doesn't follow its privacy policy.
- Expect your insurance company, agent, or any business they contract with to take reasonable steps to keep unauthorized persons from seeing, stealing, or using your personal information.
- 4. Get a notice from your insurance company, agent, or any business they contract with if an unauthorized person has (or it seems likely they have) seen, stolen, or used your personal information. This is called a *data breach*. This notice should:
 - · Be sent in writing by first-class mail or by e-mail if you've agreed to that;
 - Be sent soon after a data breach, and never more than 60 days after a data breach is discovered;
 - Describe the type of information involved in a data breach, and the steps you can take to protect yourself from identity theft or fraud;
 - Describe the action(s) the insurance company, agent, or business they contract with has taken to keep your personal information safe;
 - Include contact information for the three nationwide credit bureaus;
 - Include contact information for the company or agent involved in a data breach.
- 5. Get at least one (1) year of identity theft protection paid for by the company or agent involved in a data breach.
- 6. If someone steals your identity, you have a right to:
 - Put a 90-day initial fraud alert on your credit reports (the first credit bureau you contact will alert the other two);
 - · Put a seven-year extended fraud alert on your credit reports;
 - Put a credit freeze on your credit report;
 - · Get a free copy of your credit report from each credit bureau;
 - · Get fraudulent information related to the data breach removed (or "blocked") from your credit reports;
 - Dispute fraudulent or wrong information on your credit reports;
 - · Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;
 - · Get copies of documents related to the identity theft;
 - · Stop a debt collector from contacting you.

© 2015 National Association of Insurance Commissioners

To learn more about the protections in your state or territory, contact your consumer protection office at https://www.usa.gov/state-consumer or your state or territory's insurance department at https://www.usa.gov/state-consumer or your state or territory's insurance department at https://www.usa.gov/state-consumer or your state or territory's insurance department at https://www.naic.org/state-consumer or your state or territory's insurance department at https://www.naic.org/state_web_map.htm.

Appendix 6 – 2015 NAIC Roadmap for Cybersecurity Consumer Protections (2)

Standard Definitions under this Bill of Rights

Data Breach: When an unauthorized individual or organization sees, steals, or uses sensitive, protected, or confidential information, usually personal, financial and/or health information.

Credit Bureau (Consumer Reporting Agency): A business that prepares credit reports for a fee and provides those reports to consumers and businesses; its information sources are primarily other businesses.

Credit Freeze (Security Freeze): A way you can restrict access to your credit report and prevent anyone other than you from using your credit information.

Personal Information (Personally Identifiable Information): Any information about a consumer that an insurance company, its agents, or any business they contract with maintains which can be used to identify a consumer. Examples include:

- Full name;
- Social Security Number;
- Date and place of birth;
- Mother's maiden name;
- Biometric records; and
- Driver's license number

Helpful Links:

Credit Freeze FAQs (Federal Trade Commission) http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

Disputing Errors on Credit Reports (Federal Trade Commission) - <u>http://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports</u>

Identity Theft: What to Know, What to Do (Federal Trade Commission, May 2012). Tri-fold brochure; online PDF; can order bulk copies at no cost – <u>https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf</u>

Know Your Rights (Federal Trade Commission) - https://www.identitytheft.gov/know-your-rights.html

What Is Identity Theft? (video; Federal Trade Commission) - <u>http://www.consumer.ftc.gov/media/video-0023-what-identity-theft</u>

When Information Is Lost or Stolen (Federal Trade Commission) - https://www.identitytheft.gov/info-lost-or-stolen.html

State Consumer Protection Offices (USA.gov) - http://www.usa.gov/directory/stateconsumer/index.shtml

Directory of State Insurance Regulators (National Association of Insurance Commissioners) http://www.naic.org/state_web_map.htm

 $World's \ Biggest \ Data \ Breaches \ (information \ is \ beautiful) - \underline{http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/$

© 2015 National Association of Insurance Commissioners 2

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (1)

Model Regulation Service—4th Quarter 2017

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

- Section 2. Purpose and Intent
- Section 3. Definitions
- Section 4. Information Security Program
- Section 5. Investigation of a Cybersecurity Event
- Section 6. Notification of a Cybersecurity Event
- Section 7. Power of Commissioner
- Section 8. Confidentiality
- Section 9. Exceptions
- Section 10. Penalties
- Section 11. Rules and Regulations [OPTIONAL]
- Section 12. Severability
- Section 13. Effective Date

Section 1. Title

This Act shall be known and may be cited as the "Insurance Data Security Law."

Section 2. Purpose and Intent

- A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.
- B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Drafting Note: The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, *Cybersecurity Requirements for Financial Services Companies*, effective March 1, 2017, such Licensee is also in compliance with this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

- A. "Authorized Individual" means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems.
- B. "Commissioner" means the chief insurance regulatory official of the state.
- C. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee's possession, custody, or control.
- D. "Cybersecurity Event" means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.

^{© 2017} National Association of Insurance Commissioners

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (2)

Insurance Data Security Model Law

The term "Cybersecurity Event" does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

- E. "Department" means the [insert name of insurance regulatory body].
- F. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.
- G. "Information Security Program" means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.
- H. "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- I. "Licensee" means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.
- J. "Multi-Factor Authentication" means authentication through verification of at least two of the following types of authentication factors:
 - (1) Knowledge factors, such as a password; or
 - (2) Possession factors, such as a token or text message on a mobile phone; or
 - (3) Inherence factors, such as a biometric characteristic.
- K. "Nonpublic Information" means information that is not Publicly Available Information and is:
 - (1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee;
 - (2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements:
 - (a) Social Security number,
 - (b) Driver's license number or non-driver identification card number,

668-2

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (3)

Model Regulation Service—4th Quarter 2017

- (c) Account number, credit or debit card number,
- (d) Any security code, access code or password that would permit access to a Consumer's financial account, or
- (e) Biometric records;
- (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to
 - (a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family,
 - (b) The provision of health care to any Consumer, or
 - (c) Payment for the provision of health care to any Consumer.
- L. "Person" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.
- M. "Publicly Available Information" means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine:

- (1) That the information is of the type that is available to the general public; and
- (2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so.
- N. "Risk Assessment" means the Risk Assessment that each Licensee is required to conduct under Section 4C of this Act.
- O. "State" means [adopting state].
- P. "Third-Party Service Provider" means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain

Insurance Data Security Model Law

a comprehensive written Information Security Program based on the Licensee's Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.

B. Objectives of Information Security Program

A Licensee's Information Security Program shall be designed to:

- (1) Protect the security and confidentiality of Nonpublic Information and the security of the Information System;
- (2) Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;
- (3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and
- (4) Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.
- C. Risk Assessment

The Licensee shall:

- Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program;
- (2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;
- (3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;
- (4) Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:
 - (a) Employee training and management;
 - (b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and
 - (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and
- (5) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

Model Regulation Service—4th Quarter 2017

D. Risk Management

Based on its Risk Assessment, the Licensee shall:

- (1) Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control.
- (2) Determine which security measures listed below are appropriate and implement such security measures.
 - (a) Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;
 - (b) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;
 - (c) Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;
 - (d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;
 - (e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;
 - (f) Modify the Information System in accordance with the Licensee's Information Security Program;
 - (g) Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;
 - Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;
 - Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;

© 2017 National Association of Insurance Commissioners

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (6)

Insurance Data Security Model Law

- (j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and
- (k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.
- (3) Include cybersecurity risks in the Licensee's enterprise risk management process.
- (4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and
- (5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.
- E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

- (1) Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program;
- (2) Require the Licensee's executive management or its delegates to report in writing at least annually, the following information:
 - (a) The overall status of the Information Security Program and the Licensee's compliance with this Act; and
 - (b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.
- (3) If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.
- F. Oversight of Third-Party Service Provider Arrangements
 - (1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and
 - (2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and

668-6

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (7)

Model Regulation Service—4th Quarter 2017

secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

G. Program Adjustments

The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.

- H. Incident Response Plan
 - (1) As part of its Information Security Program, each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.
 - (2) Such incident response plan shall address the following areas:
 - (a) The internal process for responding to a Cybersecurity Event;
 - (b) The goals of the incident response plan;
 - (c) The definition of clear roles, responsibilities and levels of decisionmaking authority;
 - (d) External and internal communications and information sharing;
 - (e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
 - (f) Documentation and reporting regarding Cybersecurity Events and related incident response activities; and
 - (g) The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.
- I. Annual Certification to Commissioner of Domiciliary State

Annually, each insurer domiciled in this State shall submit to the Commissioner, a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this Act. Each insurer shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.

^{© 2017} National Association of Insurance Commissioners

Insurance Data Security Model Law

Section 5. Investigation of a Cybersecurity Event

- A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.
- B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:
 - (1) Determine whether a Cybersecurity Event has occurred;
 - (2) Assess the nature and scope of the Cybersecurity Event;
 - (3) Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and
 - (4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.
- C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.
- D. The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years from the date of the Cybersecurity Event and shall produce those records upon demand of the Commissioner.

Section 6. Notification of a Cybersecurity Event

A. Notification to the Commissioner

Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met:

- (1) This State is the Licensee's state of domicile, in the case of an insurer, or this State is the Licensee's home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or
- (2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:
 - (a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (9)

Model Regulation Service—4th Quarter 2017

- (b) A Cybersecurity Event that has a reasonable likelihood of materially harming:
 - (i) Any Consumer residing in this State; or
 - (ii) Any material part of the normal operation(s) of the Licensee.
- B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.
 - (1) Date of the Cybersecurity Event;
 - (2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;
 - (3) How the Cybersecurity Event was discovered;
 - (4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;
 - (5) The identity of the source of the Cybersecurity Event;
 - (6) Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;
 - (7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;
 - (8) The period during which the Information System was compromised by the Cybersecurity Event;
 - (9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;
 - (10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
 - (11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;
 - (12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and

^{© 2017} National Association of Insurance Commissioners

Insurance Data Security Model Law

- (13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.
- C. Notification to Consumers. Licensee shall comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.
- D. Notice Regarding Cybersecurity Events of Third-Party Service Providers
 - (1) In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 6A.
 - (2) The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.
 - (3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.
- E. Notice Regarding Cybersecurity Events of Reinsurers to Insurers
 - (1) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred.
 - (b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.
 - (2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.
 - (b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification
Appendix 7 – 2017 NAIC Insurance Data Security Model Law (10)

Model Regulation Service—4th Quarter 2017

law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner.

The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.

Section 7. Power of Commissioner

- A. The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or insurers].
- B. Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.

Section 8. Confidentiality

- A. Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.
- B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.
- C. In order to assist in the performance of the Commissioner's duties under this Act, the Commissioner:
 - May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies,

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (11)

Insurance Data Security Model Law

with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;

- (2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;
- (3) May share documents, materials or other information subject to Section 8A, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and
- (4) May enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 8C.
- E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 9. Exceptions

- A. The following exceptions shall apply to this Act:
 - (1) A Licensee with fewer than ten employees, including any independent contractors, is exempt from Section 4 of this Act;
 - (2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with, and submits a written statement certifying its compliance with, the same;

Appendix 7 – 2017 NAIC Insurance Data Security Model Law (12)

Model Regulation Service—4th Quarter 2017

- (3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.
- B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.

Section 10. Penalties

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

Section 11. Rules and Regulations [OPTIONAL]

The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.

Drafting Note: This provision is applicable only to states requiring this language.

Section 12. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 13. Effective Date

This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC).

2017 4th Quarter (adopted by Executive/Plenary via conference call)

Appendix 8 – Description and Scope of the ISO/IEC 27000 family - Information security management systems (1)

The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

There are more than a dozen standards in the 27000 family, you can see them here.

What is an ISMS?

An **ISMS** is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

It can help small, medium and large businesses in any sector keep information assets secure.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and nongovernmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

Appendix 8 – Description and Scope of the ISO/IEC 27000 family – Information security management systems (2)

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003^[2], ISO/IEC 27004^[3] and ISO/IEC 27005^[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

1 Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

Appendix 9 - The State of Insurance Fraud Technology - Current State

Current state of fraud & technology

The full scale of insurance fraud is unknown. Because this crime is designed to go undetected, the fraud-fighting community can only guess at the extent of crime and dollar losses. Fraud is perceived to be prevalent throughout the insurance lifecycle, from the application process through the claims arena. Insurers increasingly see more attempted fraud at



"point of sale" – during the application and renewal process. This is most-common with online coverage purchases. Insurers also fight internal fraud, money laundering and, for the last few years, the emerging issue of cyber fraud.

Areas employing technology. Some 76 percent of insurers said detecting claims fraud is the primary use of anti-fraud technology. That is up from 71 percent in 2014 and 65 percent in 2012. Using technology to counter underwriting and automobile rate-evasion schemes saw similar increases from 2012 to 2016. The percentage who say they use no technology in the areas listed dropped from eight percent in 2012 to 2.5 percent in 2016.

Using tech to uncover internal fraud has plateaued at 29 percent. Insurers using anti-moneylaundering software fell from 24 percent to nine percent over the last two years. The decline may

stem from the small sample size for that question in 2014.

Cyber fraud continues to be a growing issue for insurer anti-fraud departments. Nearly one of five say they use technology to combat this growing threat.



Appendix 10 – EY Major Technology Trends (1)



Appendix 10 – EY Major Technology Trends (2)

Big data and analytics	Part of the business.	evolution?	ss in data analytic	() and mode	Querantly	mprove nearly every	
	Market developments				Key questions		
	The Internet of Things, drones, social media, mobile technology and connected devices have drastically increased the data insurers can leverage across the value chain.				What are the be manage new da and gain compe	st ways to collect and ta to generate insights rtitive advantage?	
	Although insurers recognize the power of analytics to grow, optimize and protect value, many continue to be overwhelmed by the far-reaching changes required to transition to value-driven decision-making.				What cultural ar changes are neo data-driven and	nd organizational cessary to become analytics-led?	
	Leveraging data to improve underwriting and product development will drive revenues and profitability by speeding entry into profitable niches.				Which functions enhanced first?	and processes should	
Sensor data: how insurance innovators and early adopters are improving performance Sensor technology is a major contributor to big data and will profoundly change the industry. Telematics and other connected devices record driving patterns and can change behaviors. In-home and building sensors monitor environmental conditions and can revolutionize pricing and claims.							
			Sensor data us Leaders focus o	sage: leader n core busin	rs vs laggards ess capabilities		
Market and	sell	Engage customers		Differentia	te value	Model and manag	e risk
75% Laggards 28	8%	71% Laggards 27%	121	71% Laggards 2	8 9 27%	70% Laggards 24%	A
Download EY	Sensor Survey >						
Usage-based i	nsurance (UBI): welcor	ne to the new norma	ı				
UBI has gaine	d traction because it ha	s the potential to ge	nerate substantia	al benefits, ir	ncluding:		_
40% 40%	Reduction in clain Reduction in polic	ns cost administration co	ost S	• 1 • 5	More effective polic Substantially lower	cy pricing r acquisition costs	3

Appendix 10 – EY Major Technology Trends (3)

Legacy system transformation	Digital and omnichannel InsurTech and blockchain	Big data and analytics	Cybersecurity	
	From modernization to mobile	e to robots - where are you or	the journey?	
	Core insurance systems are la reduce costs. "Robots" are se development is called robotic	being modernized at scale to oftware tools that simplify bus o process automation (RPA).	optimize processes, increas iness processes, and the tea	e collaboration and chnology behind this
	Market developments		Key questions	5
	Management and the second second second	1	1400 and a star of	

Many carriers have purchased modern, "rules and tools" core systems over the past five years.	What's the right level of standardization and out-of-box product capability to reduce total cost of ownership?
With a single line of business or geography up and running, most carriers are looking to extend these tools across the business to leverage their investments.	How do you demonstrate the business impact of core transformation efforts to scale up implementation?
Insurers embrace outsourcing, robotic process automation and SaaS solutions to reduce costs.	What's the best way to embrace new technologies to react quickly without extensive recoding and reconfiguring existing systems?
Insurers are investing to extend their core applications and systems platforms via customer-facing and agent-facing portals and apps.	Which back-office systems can be used to enhance front-line interactions?
Software robots can mimic human actions and automate repetitive tasks across multiple business applications without altering existing infrastructure and systems, while improving productivity, cycle times, accuracy and compliance.	Which functions or processes are best suited to initial deployments of robotic process automation?
The evolution of automation	

EY -	EY - The evolution of automation				
	Manual Execution	Scripting	Orchestration	Autonomics (RPA)	Cognitive
Attributes	Manual One-off Non-repeatable	Tasks Linear Standard Repeatable	Activities Orchestrated Complex Standard Multi-scripted	 Processes Dynamic Non-standard Contextual Inference 	Self-aware Predictive Self-learning Self-healing
		Current State		Target State	Future State
	Labor efficiencies			Labor eli	mination
Source: Institute for Robotic Process Automation. EY					

Appendix 10 – EY Major Technology Trends (4)



Appendix 10 – EY Major Technology Trends (5)



Appendix 11 – Accenture – Technology Vision Trend Evolution



Technology Vision trend evolution

00-DAY PLAN

1

2

3

4

5

6

7

8

1

2

3

(4)

(5)

Rank your customer, intermediary and employee interactions by how critical they are to your current revenue and future growth.

Pick three to five interactions and work with your service and product teams to streamline customer engagement with your most valued products and services; launch a test-and-learn process.

Launch a discovery phase to analyze how robotics and Al could bring strategic value to your organization.

Identify what information and insights you lack that would help you improve the user experience.

Develop AI personas that fit your brand and communicate your brand voice.

Consider piloting Al in roles like content curator (for personalization) or interaction advisor (for intelligent automation). Think about starting with an internal process such as IT support.

Identify communication channels and platforms for integrating conversational experiences with your brand. Consider internal as well as external interactions.

Gather and review existing key performance indicators (KPIs) for customer success. Ensure these KPIs account for the benefits of simplified interactions.

365-DAY PLAF

Implement increasingly sophisticated AI personas that not only curate or advise, but also aim to orchestrate as much as possible—among your brand and ecosystem stakeholders—for key customer interactions.

Create a robotics and AI center of excellence to industrialize and scale-up your robotics and AI projects.

Develop analytics that takes account of front-end customer insights and back-end business intelligence to better understand key customer interactions.

Develop and pilot a training program for AI teams and UX/ UI teams to cross-train on implementing AI to improve and simplify key customer interactions.

Design a new customer journey where AI serves as your frontline brand ambassador for customer service interactions, communications, and engagements with customers.

Appendix 12 – Accenture – 100 Day and 365 Day Plan – Trend 2. Ecosystem Power Plays (2)

100-DAY PLAN

6

Conduct an audit identifying how many internal and external platforms your company is using and the goals for their use. Identify and address unnecessary overlaps.

Determine the platforms your organization most relies on, as well as those that most depend on you. These are the ecosystems where your organization should hold its strategic and market strengths.

Have a strategy summit with your closest partners to understand their goals for the future. Uncover shared goals and commit to developing a strategic plan for achieving them together.

Evaluate your options—build an ecosystem around a customer need (transport, healthcare) or participate in someone else's. Make the choice based on customer lifecycle events and the insurer's role.

Consider your organization's future through the lens of the biggest disruptions shaping your market. Craft the ideal role of your company in this future, and develop a shortlist of partners who can help make it a reality.

Develop metrics to quantify the results of ecosystem participation. These may include sales growth, API requests, customer satisfaction and growth of new partnerships.

Extend a significant portion of a core business function to a third-party platform or digital aggregator. Build a bigger stake in an emerging ecosystem, bringing its strengths into your organization.

Use an existing partnership to pilot building your own ecosystem. Make your selection based on complementary strengths, like mature platforms or digital services. Start with one joint offering, such as combining services into a single point of access.

Prepare a foundation for expanding your ecosystem by making a significant investment in either a startup or a joint venture that will establish a foothold in an area critical to your organization's transformation.

Appoint a cross-functional team and C-suite sponsor to guide long-term ecosystem efforts.



100-DAY PLAN

1

2

3

4

5

Task a talent marketplace transformation sponsor to define a company-wide talent marketplace strategy, and to establish measurable goals for improving agility and workforce opportunities.

Launch a cross-functional team to define governance and HR policy, identify the relevant and allowable technology tools, and manage legal issues for your corporate blended workforce strategy.

Start identifying pilot opportunities by interviewing business leaders within your organization to determine which groups, projects, or products are most in need of gaining agility in their workforce and skills.

Establish key performance indicators to track how the talent marketplace transformation is advancing broader business priorities for your organization. Communicate these data points with stakeholders on a regular basis.

Engage with freelance labor platform providers as your potential partners for pilots. Start understanding their knowhow, offerings, and enterprise customer success stories.

365-DAY PLAN

Home in on areas of the business where the work is already remote, externally sourced, highly variable, cost sensitive, or driven by specialist skills. Use this as a first pilot to engage external freelance labor markets and platforms.

Launch an internal competition to be the first group to assemble a team entirely from an internal labor marketplace. Track the progress of this team, capture lessons learned throughout the process, and share them with internal stakeholders. Launch a slightly larger second phase. Continue to iterate and expand.

With lessons learned from both pilots, define a formal governance structure to manage freelance worker policies and best practices.

Armed with a formal governance structure, policies, and best practices, work toward blending the internal and external strategies with a goal of erasing the boundaries between the internal organization and the external ecosystem of labor platforms.

Appendix 12 – Accenture – 100 Day and 365 Day Plan – Trend 4. Design for Humans (4)



Enumerate the journeys your customers and employees take with your company, products, and/or services. Indicate the points on these journeys where engagement with your company begins and ends.

Identify the human behaviors that contribute to positive and negative outcomes customers or employees experience when interacting with your technology channels.

Catalog the data you already collect, could collect (but presently do not), and cannot currently collect that offers insight into customer behaviors and decision-making.

Using the customer behavior insights that you currently possess, plan a pilot to offer a behavior-personalized experience with an existing product or service.

To support conducting behavior-based A/B research with customers, draft a code of data ethics for such experiments.

Establish a strategic vision for making your technology products and services more goal-oriented.

Identify at least three business cases for for maximizing behaviors that promote positive outcomes in existing and upcoming products.

Using the journeys previously enumerated, work with strategy and product teams to uncover opportunities for improving the quality of outcomes that customers and employees receive with your company's guidance.

Identify key organizations that engage with your customers or employees before and after your company's role on each journey. Establish data sharing agreements with these organizations to further enrich your business's understanding of behavior across a journey.

Finalize your code of ethics and begin performing behavioral studies to understand and improve the ways your technology elicits, or fails to elicit, specific human behaviors.

Challenge product teams to use behavioral insights to help individuals realize unique goals.

)O-DAY PLAN 3 4 365-DAY PLAN

1

2

5

1

2

3

4

Create a stakeholder map for each industry in which your company operates and catalog the ecosystems within these industries.

Make a list of ways your products and services influence society. Build a conscious strategy for influencing the social contract with a governance structure that ensures responsible and ethical influence.

Take inventory of data inputs to your organization. Focusing on areas where you receive personally identifiable information (PII), or where metadata could generate PII, enumerate the potential risks to highlight areas where new governance may be needed.

Highlight areas of innovation you're engaged in where improving or updating government regulation or industry / ecosystem rules would help to encourage innovation or economic growth.

Create a team to work with regulators at local, regional, and/or national levels. Efforts should focus on education, information sharing, and responsible growth of new industries.

Using the ecosystem catalog, identify the intersection of the industries you operate within, where you're growing, and which ones have the most opportunity for new ecosystems. Build a strategy for starting a new ecosystem to complement and accelerate your growth into new markets.

Publish your governance model for public inspection, and begin implementing your strategy. Concentrate on recognizing the influence you already have and optimize for the behaviors you want to encourage.

From your data input inventory, pilot systems that make use of embedded-governance technologies: differential privacy, homomorphic encryption, and blockchain-based solutions.

Select a single initial area of innovation to engage with government regulators. Begin with individual conversations with multiple stakeholders.

BIBLIOGRAPHY

- 1. Aruda W., 5 Great Companies That Get Corporate Culture Right. In Forbes 2017, https://www.forbes.com/sites/williamarruda/2017/08/17/5-great-companies-that-getcorporate-culture-right/#9e48abc15828
- Baskerville R., Spagnoletti P., Kim J., Incident-centered information security: Managing a strategic balance between prevention and response, "Information & Management" Vol. 51 Issue 1, 2014, p. 138-151
- Baskerville R., Dhillon G., Information Systems Security Strategy: A Process View. In D.W. Straub, S. Goodman, R. Baskerville (Eds.), Information Security: Policy, Processes, and Practices, New York 2008
- BITAG Broadband Internet Technical Advisory Group Internet of "Things" (IoT) Security and Privacy Recommendations, Broadband Internet Technical Advisory Group, Inc., 2016, http://www.bitag.org/documents/BITAG_Report_Internet_of_"Things"_ (IoT)_Security_and_Privacy_Recommendations.pdf
- Bjarnason E., Hauser C., Iceland Makes Companies Prove They're Not Paying Women Less. In New York Times, 2018, https://www.nytimes.com/2018/01/03/world/europe/ iceland-equal-pay.html?_r=0
- 6. Bort J., *Netflix Employees Are Happier With Their Job Than Facebook or Google Employees*. In Inc. 2017, https://www.inc.com/business-insider/tech-employees-anony-mously-rate-companies-work-facebook-google-netflix-twitter.html
- Carter M., Thompson N., Crampton P. et al., Workplace bullying in the UK NHS: a questionnaire and interview study on prevalence, impact and barriers to reporting, "BMJ open", 2013, 3(6), e002628
- Cglar D., Tozun G., Karay M., Mobbing Behaviors in Public and Private Banking Sector: A Case Study in Northern Cyprus, "International Journal of Economic Perspectives", 2017, Vol. 11 Issue 2, p. 76
- 9. Chappell D., Di Martino V., *Violence at work*. International Labour Organization, Geneva 2006, http://www.ilo.org/wcmsp5/groups/public/%40dgreports/%40dcomm/%40publ/documents/publication/wcms_publ_9221108406_en.pdf

- 10. Cisneros V., *Mobbing in Spanish public administrations* report. Courtesy of Iñaki Piñuel to the authors
- 11. coalition-against-insurance-fraud-the-state-of-insurance-fraud-technology-105976.pdf
- 12. Coetzee M., van Dyk J., Workplace Bullying and Turnover Intention: Exploring Work Engagement as a Potential Mediator, "Psychological Reports", 2018, Vol. 121(2), p. 376
- Crawford D., Chaffin C., Scarborough S., *Effective Compliance Systems: A Practical Guide for Educational Institutions* Institute of Internal Auditors, 2001, https://www.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/Higher_Ed/2008/ Mon/RiskAssessmentMatrixQuickReference.pdf
- 14. Creating a safe work environment. Best practices to deal with sexual harassment at the work place. A. Deloitte India survey report, 2016, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-anti-sexual-harassment-report-noexp.pdf
- 15. cybersecurity.ieee.org/blog/2016/02/17/wearfitsecurity-design-analysis-of-a-wearable-fitness-tracker/
- 16. European Directive 2002/73/EC.Source: European Parliament, 2002a
- 17. French K., Agars M., *Work–Family Culture in Low-Income Environments*, "Journal of Career Development", 2018, Vol. 45 Issue 1, p. 50-67
- Fu K., Infrastructure Disruption: Internet of "Things" Security, Testimony before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing, and Trade, 2016, https://energycommerce.house.gov/hearings-and-votes/hearings/ understanding-role-connected-devicesrecent-cyber-attacks
- Gehani A., Tariq D., Baig B., and Malik T., *Policy-Based Integration of Provenance Metadata*, 12th IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 2011
- 20. http://ec.europa.eu/justice/grants/results/daphne-toolkit/en/daphne-toolkit-%E2%80%93-active-resource-daphne-programme
- 21. http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html
- 22. http://understandinsurance.com.au/insurance-fraud
- 23. http://worldpopulationreview.com/us-cities/atlanta-population/
- 24. http://www.europarl.europa.eu/hearings/20071121/femm/framework_agreement_en.pdf
- 25. http://www.ey.com/gl/en/industries/financial-services/insurance/ey-tech-trends
- 26. http://www.helpstopfraud.org/What-is-Insurance-Fraud/Impact#
- 27. http://www.hse.gov.uk/statistics/causinj/violence/work-related-violence-report-2018.pdf
- http://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---actrav/documents/publication/wcms_546645.pdf (Violence and harassment against women and men in the world of work: trade union perspectives and action / International Labour Office, Bureau for Workers' Activities (ACTRAV). – Geneva: ILO, 2017.)

- 29. http://www.lawyersmutualnc.com/blog/profile-of-a-fraudster
- 30. http://www.naic.org/documents/committees_ex_cybersecurity_tf_160524_draft_ins_data_sec_model_law.pdf
- 31. http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_ cybersecurity_consumer_protections.pdf
- 32. http://www.naic.org/store/free/MDL-668.pdf
- 33. http://www.un.org/womenwatch/daw/cedaw/cedaw.htm
- 34. http://www.unaids.org/en/resources/fact-sheet
- 35. https://cdn2.hubspot.net/hubfs/524149/Gated_Content/financial%20white%20 paper%202017%20FINAL%20Pages.pdf?submissionGuid=94df83ac-02df-41dc-ba2f-2e0c179ae533
- 36. http://us.generaliglobalassistance.com/blog/white-paper-impact-cybersecurity-incidents-financial-institutions/
- 37. https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf
- 38. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- 39. https://definitions.uslegal.com/s/soft-law
- 40. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulationgdpr-govern_en
- 41. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0043
- 42. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0073
- 43. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01. ENG
- 44. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML
- 45. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0078: en:HTML
- 46. https://kasisto.com/kai-banking/on-mobile/
- 47. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf
- 48. https://rm.coe.int/16806f53e6
- 49. https://wall-street.com/impact-cyber-attacks-banking-industry/
- 50. https://www.accenture.com/_acnmedia/Accenture/next-gen/top-ten-challenges/challenge9/pdfs/Accenture-2016-Top-10-Challenges-09-Cyber-Security.pdf#zoom=50
- 51. https://www.accenture.com/us-en/insight-insurance-technology-vision-2017
- 52. https://www.bls.gov/iif/oshwc/cfoi/workplace-homicides.htm
- 53. https://www.bluefin.com/bluefin-news/global-cybersecurity-laws-regulation-chang-es-2018/

- 54. https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/
- 55. https://www.criminaldefenselawyer.com/crime-penalties/federal/Insurance-Fraud.htm
- 56. https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018-business-view-security/
- 57. https://www.eeoc.gov/laws/types/
- 58. https://www.europol.europa.eu/newsroom/news/atm-raiders-jailed-in-joint-cross-border-investigation
- 59. https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf
- 60. https://www.forbes.com/sites/forbestechcouncil/2018/03/28/blockchain-what-is-it-and-what-is-it-for/#6148623a1a16
- 61. https://www.forbes.com/sites/mikescott/2018/03/07/energy-industry-worried-about-cyber-attacks-but-doesnt-reallyknow-what-to-do/#774f405a68bb
- 62. https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb
- 63. https://www.greentechmedia.com/articles/read/energy-sector-ups-cyber-security-amid-growing-it-threats#gs.OXgDL6U
- 64. https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYea rEndReview.pdf
- 65. https://www.insuranceeurope.eu/about-us
- 66. https://www.insuranceeurope.eu/sites/default/files/attachments/The%20impact%20 of%20insurance%20fraud.pdf
- 67. https://www.insureon.com/about-us/insurtech
- 68. https://www.investopedia.com/terms/i/insurtech.asp
- 69. https://www.iso.org/isoiec-27001-information-security.html
- 70. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks/
- 71. https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/12
- 72. https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-thethreat-that-inspires
- 73. https://www.npr.org/2012/03/22/149099866/cybersecurity-bill-vital-need-or-just-more-rules
- 74. https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-weekby-cyber-attack
- 75. https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity-regulatory-issues-in-theinsurance-industry-protiviti.pdf
- 76. https://www.protiviti.com/US-en/insights/security-threat-report
- 77. https://www.rgare.com/docs/default-source/newsletters-articles/fraud-white-paper. pdf?sfvrsn=a7ffa688_0

- 78. https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018
- 79. https://www.safeworkaustralia.gov.au/system/files/documents/1702/psychosocial-bullying-statement.pdf
- 80. https://www.slideshare.net/reed2001/culture-1798664/4-Seven_Aspects_of_our_Culture
- 81. https://www.the-digital-insurer.com/blog/10-insurtech-trends-insurance-2018/
- 82. https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-nowsays-more-than-five-million-fingerprints-compromised-in-breaches/?utm_ term=.0d67db3857ea
- 83. https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyberattacks/
- 84. https://www.wsj.com/articles/why-we-have-to-really-worry-about-the-banks-cybersecurity-1513652881
- 85. https://www2.deloitte.com/be/en/pages/risk/articles/insurance.html#
- 86. IFREI website: http://ifrei.iese.edu/en/
- 87. ILO Convention
- Jacobson R.K., Eaton A.A., How Organizational Policies Influence Bystander Likelihood of Reporting Moderate and Severe Sexual Harassment at Work, "Employee Responsibilities & Rights Journal", 2018, Vol. 30 Issue 1, p. 37-62
- 89. Japan Labor Flash, 2003. Cited in Chappell D. and Di Martino V., *Violence at work*, International Labour Organization 2006
- Madera J.M., When Targets Blame Their Organization for Sexual Harassment: A Multilevel Investigation of Within-Person Appraisals, "Cornell Hospitality Quarterly", 2018, Vol. 59 Issue 1, p. 49-60
- 91. Malik T., Nistor L., Gehani A., *Tracking and Sketching Distributed Data Provenance*, 6th IEEE International Conference on e-Science, 2010
- 92. Mumel D., Jan S., Treven S., Malc D., *Mobbing in Slovenia: Prevalence, mobbing victim characteristics, and the connection with post-traumatic stress disorder*, "Our Economy", 2015, Vol. 61 Issue 1, p. 3-12
- 93. Nami G., Nami R.F., *The bully-free workplace: Stop jerks, weasels, and snakes from killing your organization,* John Wiley & Sons Inc. Hoboken, New York, 2011
- 94. National Research Council. Accelerating Technology Transition: Bridging the Valley of Death for Materials and Processes in Defense Systems. Washington, DC: The National Academies Press, 2004
- 95. PwC Getting ahead of the watchdogs: Real-time compliance management 2018 State of Compliance, 2018, https://www.pwc.com/us/en/risk-assurance/state-of-compliance-study/assets/pwc-2018-state-of-compliance.pdf
- Romanescu M.L., Mobbing Phenomenon Factors of Discrimination and Stress, "Annals of the Constantin Brâncuşi University of Târgu Jiu, Economy Series", 2017, Issue 1/2017, p. 124

- 97. SEAT *Code of Conduct* (Spanish version), http://www.seat.es/content/dam/countries/es/ corporate/codigo-de-conducta/pdf-codigo-de-conducta/codigo-de-counducta.pdf
- 98. Thompson C., Beauvais L., Lyness K., When Work-Family Benefits Are Not Enough: The Influence of Work-Family Culture on Benefit Utilization, Organizational Attachment, and WorkFamily Conflict, "Journal of Vocational Behavior", 1999
- 99. Thomson Reuter, *The advantages of a global compliance training solution*, https://risk. thomsonreuters.com/en/products/online-compliance-training.html
- 100. Violence at work, ILO CH1
- 101. West J. et al., *WearFit: Security Design Analysis of a Wearable Fitness Tracker*, IEEE Cyber Security, 2016
- 102. Yahyaoui Krivenko E., The Role and Impact of Soft Law on the Emergence of the Prohibition of Violence Against Women Within the Context of the CEDAW. In Tracing the Roles of Soft Law in Human Rights, 2016, p. 47-67
- 103. York K., *Dyn Statement on 10/21/2016 DDoS Attack*, 2016, http://dyn.com/blog/dyn-statementon-10212016-ddos-attack/

LIST OF FIGURES AND TABLES

LIST OF FIGURES

Figure I.1.	Cyberthreat awareness and preparedness	27
Figure I.2.	Overview of types of cyberattacks and data breaches	28
Figure I.3.	Top operational risks for 2018	31
Figure I.4.	2016 financial fraud losses by type	32
Figure II.1.	Fraudster Profile	36
Figure II.2.	Soft and Hard Insurance Fraud	37
Figure II.3.	Cybersecurity regulation: Call to Action	40
Figure II.4.	Cybersecurity innovation: Call to Action	41
Figure II.5.	Five Major Technology Trends	42
Figure II.6.	Accenture – The Era of the Intelligent Insurer	44
Figure II.7.	Interaction of Two Paradigms	46
Figure IV.1.	Offences Against the Rights of People in Paid Work in Poland	70
Figure IV.2.	Records of cases related to discrimination in Polish Regional Courts: Total resolving in 2016/17	70
Figure IV.3.	Percent included from the total resolving in 2016/17	71
Figure IV.4.	Number of incidents of violence at work for adults of working age in employment 2007-2017 (CSEW)	72
Figure IV.5.	Percentage of violence at work incidents by injury type 2016/17 (CSEW)	72
Figure IV.6.	Employment rate for men and women, % of working age population, Q1 2018	79
Figure IV.7.	Gender wage gap, % of male median wage, 2016	79
Figure IV.8.	Employment rate by age group, % in same group age, Q1 2018	80
Figure V.1.	Relationship between data, information, and knowledge	103
Figure V.2.	The VIVID display of current cybersecurity status of a protected (virtual or real) private network	120

Figure V.3.	The current sources of infection and cyberattack	121
Figure V.4.	Representative DATES architecture. The defended system is instrumented with detection and correlation DATES solutions to produce a situational awareness framework that is effective against ICS-specific attacks	124
Figure V.5.	Initial enrollment in a cryptographically secured BIA system	131
Figure V.6	Identification and authentication in a cryptographically secured BIA system	131
Figure V.7.	BlockCIS overview	134
Figure V.8.	BlockCIS node deployed at an insured entity's network	135
Figure V.9.	BlockCIS node deployed at the insurer's side	135
Figure V.10.	Third party services involvement in BlockCIS	135
Figure V.11.	BotHunter's malware infection dialog model	142
Figure V.12.	BotHunter's malware infection dialog model	143
Figure V.13.	The Valley of Death Between Research and Industry	153
Figure V.14.	Cybersecurity R&D Execution Model for Technology Transition	156
Figure V.15.	SRI's 5 Disciplines of Innovation. All must be present	
	for success	159

LIST OF TABLES

Table II.1.	Features Distinguishing Prevention Models from Response Models	45
Table II.2.	Summary of Information Security Management Theories and Characteristics	47
Table III.1.	Attacker Categories for ICS	60
Table III.2.	Security Controls for ICS	62
Table IV.1.	What Constitutes Physical Violence	71
Table IV.2.	Experiences of Physical Violence – example	71
Table IV.3.	Deadly Consequences of Psychological Violence	72
Table IV.4.	Definition and Types of Sexual Harassment	74
Table IV.5.	Consequences of Bullying	75
Table IV.6.	Experiences of Bullying	75
Table IV.7.	Findings in the Mobbing Arena	77
Table V.1.	Research questions involving behavioral aspects of cybersecurity	116
Table V.2.	Participant in BlockCIS Instantiation Using Hyperledger	138
Table V.3.	Assets and Access Rights in BlockCIS Instantiation	
	Using Hyperledger	139
Table V.4.	What to do and not do in R&D Technology Transition	162

LIST OF APPENDICES

Community Gold Standard – Overarching Capabilities Definitions	165
Community Gold Standard – Capabilities Definitions	171
Community Gold Standard Best Practices Tool Kit (Link)	194
Insurance Europe: Combating fraud	197
Deloitte Case Study	200
2015 NAIC Roadmap for Cybersecurity Consumer Protections	203
2017 NAIC Insurance Data Security Model Law	205
Description and Scope of the ISO/IEC 27000 family - Information	
security management systems	218
The State of Insurance Fraud Technology – Current State	220
EY Major Technology Trends	221
Accenture – Technology Vision Trend Evolution	226
Accenture – 100 Day and 365 Day Plan	227
	Community Gold Standard – Overarching Capabilities Definitions Community Gold Standard – Capabilities Definitions Community Gold Standard Best Practices Tool Kit (Link) Insurance Europe: Combating fraud Deloitte Case Study 2015 NAIC Roadmap for Cybersecurity Consumer Protections 2017 NAIC Insurance Data Security Model Law Description and Scope of the ISO/IEC 27000 family – Information security management systems The State of Insurance Fraud Technology – Current State EY Major Technology Trends Accenture – Technology Vision Trend Evolution Accenture – 100 Day and 365 Day Plan





Projekt *Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości,* współfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Raport jest pierwszym tego typu opracowaniem w polskim piśmiennictwie, szczególnie w tak oryginalnym i profesjonalnym ujęciu. [...] Integralną i niezwykle ważną dla percepcji raportu część stanowią załączniki, które poszerzają zakres wiedzy zawartej w opracowaniu, ułatwiając jej zrozumienie. [...] Raport zawiera autorskie ujęcie zjawiska relatywnie nowego w praktyce życia gospodarczego i proponuje zasady oraz metody zarządzania nim. Charakteryzuje się właściwym, interdyscyplinarnym podejściem. Napisano go na podstawie aktualnej – głównie angielskiej – literatury oraz z wykorzystaniem badań własnych autorów. Odpowiada na pilne i rosnące zapotrzebowanie praktyki gospodarczej. Jest innowacyjną pozycją na polskim rynku wydawniczym.

> PROF. DR HAB. BOHDAN JELIŃSKI Uniwersytet Gdański

Praca jest oryginalnym osiągnięciem naukowym, wypełniającym lukę w słabo zbadanym jak dotąd obszarze zapobiegania przestępczości w sektorach: finansowym, ubezpieczeniowym i energetycznym oraz w obszarze zarządzania zasobami ludzkimi. Proponowane rozwiązania przyczynią się do poprawy skuteczności działania w analizowanych sektorach.

> PŁK DR HAB. TOMASZ KOŚMIDER, PROF. ASW Akademia Sztuki Wojennej w Warszawie

Raport prezentuje innowacyjne rozwiązania w kwestii zarówno produktów zapobiegających przestępczości, jak i procesów zarządczych przedstawionych w szczególności w rozdziale dotyczącym zarządzania ludźmi. Opracowanie ukazuje również, z jakimi wyzwaniami natury prawnej może mierzyć się w przyszłości ustawodawca na szczeblu krajowym i ponadnarodowym, w tym unijnym. [...] Raport może przyczynić się także do podjęcia dalszych badań nad cyberprzestępczością w Polsce.

> DR HAB. KRYSTYNA NIZIOŁ, PROF. US Uniwersytet Szczeciński

